[OSSA-2020-002] Unprivileged users can retrieve, use and manipulate share networks (CVE-2020-9543)

Bug #1861485 reported by Tobias Rydberg on 2020-01-31

This bug affects 1 person 268

Affects	Status	Importance	Assigned to	Milestone
OpenStack Shared File Systems Service (Manila)	Fix Released	High	Mohammed Naser	OpenStack Shared File Systems Service (Manila) ussuri-3

Bug Description

If a user (any user of any tenant) know the ID of someone else's share-network, they can show that share-network, create shares on that share-network and also delete that share-network.

The share-network of the unknown tenant that I know the ID for will not be show while doing a `manila share-network-list`.

But for example, doing a `manila share-network-delete <id of any share-network belonging to another tenant>` will be accepted and share network will be deleted.

Tags: in-stable-pike in-stable-queens in-stable-rocky in-stable-stein in-stable-train

CVE References

2020-9543

Mohammed Naser (mnaser) wrote on 2020-01-31: #1

I can confirm this as well on my side. The reason is that there is absolutely no checks for ownership here:

https://github.com/openstack/manila/blob/master/manila/api/v2/share_networks.py#L60
https://github.com/openstack/manila/blob/master/manila/api/v2/share_networks.py#L79

I'm working on some tests that fix this and will post them privately.

Tom Barron (tpb) wrote on 2020-01-31: #2

Thanks for finding this, Tobias, and thanks for work on a fix, Mohammed!

Changed in manila:
status:New → Confirmed
importance:Undecided → High
milestone:none → ussuri-3
assignee:nobody → Mohammed Naser (mnaser)

Mohammed Naser (mnaser) wrote on 2020-01-31: #3

0001-share_networks-enable-project_only-API-only.patch (7.0 KiB, text/plain)

The following is a patch against master that fixes this, including tests and passing all tests and pep8.

Mohammed Naser (mnaser) wrote on 2020-02-06: #4

Any progress on this, please? :)

Mohammed Naser (mnaser) wrote on 2020-02-10: #5

I added Magnus as I've worked with him here on this issue.

Tom Barron (tpb) wrote on 2020-02-19: #6

The fix looks reasonable to me. Goutham?

Tom Barron (tpb) wrote on 2020-02-19: #7

Just to make sure I understand the impact, though, IIUC the vulnerability here requires that one be able to guess the UUID for another project's share-network. To quote Jeremy Stanley from another issue: "If it comes down to guessing, that's considered generally impractical. Wikipedia suggests brute-forcing a specific version 4 UUID would involve trying "1 billion UUIDs per second for about 85 years ..." https://en.wikipedia.org/wiki/Universally_unique_identifier#Collisions

Or am I missing something and there's a practical way to get the UUIDs for share-networks belonging to other projects?

Note that I'm not against fixing this and as I said the fix looks good to me ...

Mohammed Naser (mnaser) wrote on 2020-02-19: #8

I think the thing that might be worry-some is the fact that users may expect that their UUIDs are not anything that can cause issue to be shared publicly (say, if I put it inside a git repo) and there is a potential in someone taking advantage of that technically.

Goutham Pacha Ravi (gouthamr) wrote on 2020-02-22: #9

Tobias thank you for reporting this bug; and thanks Mohammed for the patch. I reviewed and tested the change and it looks appropriate to me.

To be able to view details on a resource that's owned by another project is one thing, but to manipulate the resource is more severe. I agree the user expectation is that UUIDs aren't harmful by themselves and can be divulged.

Is there a security team guidance that this class of issues does not warrant being a security issue? If not, I am inclined to confirm this as a significant vulnerability for multi-tenant clouds.

Goutham Pacha Ravi (gouthamr) wrote on 2020-02-22: #10

@fungi: Can you please take a look and help us understand if we should follow the VMT process [1] to treat this bug?

[1] https://security.openstack.org/vmt-process.html

Jeremy Stanley (fungi) wrote on 2020-02-22: #11

"UUID guessing" is the classic example for what the OpenStack VMT considers impractical to exploit (class C1):

https://security.openstack.org/vmt-process.html#incident-report-taxonomy

There are lots of security mechanisms we rely on which boil down to assuming an attacker can't guess absurdly long numbers. This particular classification came about because there are, in particular, numerous services in OpenStack which assume UUIDs are treated as secret information. The usual tactic we take with a class C1 report is to switch it to public as a security hardening opportunity, and optionally, if it represents a notable risk, draft an OpenStack Security Note (considered an addendum to the Security Guide) warning users and deployers of this particular risk so they can be more aware of it.

Jeremy Stanley (fungi) wrote on 2020-02-22: #12

This discussion sounded very familiar by the way... I suspect 1861895 (also still private for the momenr) is a duplicate.

Goutham Pacha Ravi (gouthamr) wrote on 2020-02-25: #13

Hi Jeremy,

Thank you for the clarification and a link to the taxonomy. While it is going to be unlikely that the UUIDs can be guessed; the impact here would be more if the UUIDs can be obtained via other means, such as sniffing the network packets or capturing network data coming from an insecure client. The Share Network UUIDs are there in the URL, and so if an attacker gets access through those means, can manipulate the resource in undesirable ways. We did not design for these IDs to be secret information.

Examples of the Share Network UUIDs in APIs:

https://docs.openstack.org/api-ref/shared-file-system/#show-share-network-details
https://docs.openstack.org/api-ref/shared-file-system/#update-share-network
https://docs.openstack.org/api-ref/shared-file-system/#add-security-service-to-share-network
https://docs.openstack.org/api-ref/shared-file-system/#delete-share-network

Example of Share Network UUIDs in Horizon Dashboard URLs:

Share Network details page:
http://127.0.0.1/dashboard/project/share_networks/0b0fc320-d4b5-44a1-a1ae-800c56de870c

Could you please advise if we should still consider this a class C1 security vulnerability?

Regarding LP 1861895, I am unable to reproduce the issue locally. I'll comment on that bug, it's very likely that an insecure default policy is allowing that vulnerability.

Jeremy Stanley (fungi) wrote on 2020-02-25: #14

Ahh, thanks for the clarification. On closer inspection I see that 1861895 was about unintended access via guessed share UUIDs and this report is about share-network UUIDs.

At any rate, it sounds like leveraging this issue would require another vulnerability (in the browser, the connection, the client's system...) or some degree of social engineering, as Manila doesn't disclose these UUIDs to users for other tenants than those with which the resources are associated. It seems like a low enough in risk that you could fix it in public without any embargo, and could warrant an accompanying CVE assignment, though whether you consider this a serious enough breach of Manila's security model to issue an advisory or to just treat it as a security hardening opportunity is up to you.

Goutham Pacha Ravi (gouthamr) wrote on 2020-02-28: #15

Hi Jeremy, all,

After an discussion with those involved, we concluded to follow the VMT guidelines for this one for two reasons:

The seriousness of the issue and possible attack vectors:
 * attackers being able to view share network details
 * attackers creating shares and share groups on share networks
    (clobbering namespace of a different tenant causing denial of
    service - manila does not provide any way for attackers to
    connect to these resources and utilize them in a meaningful
    way to create other kinds of damage)
 * attackers being able to manipulate share networks - create or

Michael Rowland H...
Mika Kohonen
Mohankumar
Naved Ali
Naved Ali Shah
Paul Voccio
Pavani_addanki
Perry Waldner
Pradeep Kumar Singh
Pradeep Roy Kandru
Prateek
Pushpa Datla
Raju Alluri
Ranjit Ray
Richa
Rick Melick
Rohini Diwakar
Ron Cannella
Ryo Shi
Satyanarayana Pat...
Shangzhong Zhu
Shawn Hartsock
Shruthi Chari
Sid Sun
Songhee Kang
Soo Choi
Steve Sloka
Steven Pavlon
Stuart Hart
Tao Zhou
Taurus Cheung
Tayaa Med Amine
Tiago Everton Fer...
Tom Barron
Tushar Patil
Uma
Vida Haririan
Vidhisha Nair
Vinu Pillai
Xin Zhong
Xing Yang
Yongqiang Yang
Zahid Hasan
ZhangNi
Ziv
ammarun
avinashsau
baijiaruo
brightson
bugtracker@devshe...
cargonza
chaiwat wannaposop
chitu
congge
fei Yang
gsccc
iopenstack
iswarya vakati
jason bishop
jay.xu
jeff wang
kalim khuang
kgrvamsi
lanpi
laoyi
liaonanhai
lololmarwa255
lpmqtt
maestropandy
manish
mershard frierson
miralaunchpad
mohit.048
monika
nawawit kes
raja
satyanarayana pat...
satyanarayana pat...
sivagnanam C
tangfeixiong
vivek.ys
xiaoningli
xreuze
yangbo
yangzhenyu

Patches

0001-share_networks-enable-project_only-API-only.patch

delete share network subnets, update share network metadata and
delete share networks

the Manila team has expressed interest to submit an application
for the "vulnerability-managed" tag and I will begin working on the
process. Handling this bug through the full VMT process allows us to
gather experience to deal with future issues.

I have submitted a request for a CVE to be assigned for this bug. The next
steps are as follows:

- Embargoed Disclosure [3] (Timeline: 3-5 business days): I will begin
this as soon as
I hear back from MITRE.
- Disclosure: propose mnaser's patch upstream to master and all open
stable branches, fast track approvals
- Send an OSSA to the Openstack-discuss ML

Thanks for your inputs. Please let me know if you have any further
comments regarding this.

Patch file for master/ussuri (March 2nd 2020)

Patch file for stable/train (March 2nd 2020)

Patch file for stable/stein (March 2nd 2020)

Patch file for stable/rocky (March 2nd 2020)

Patch file for stable/queens (March 2nd 2020)

Patch file for stable/pike (March 2nd 2020)

Add patch

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #16

Patch file for master/ussuri (March 2nd 2020) (7.0 KiB, text/plain)

Patch file for master (March 2nd 2020)

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #17

Patch file for stable/train (March 2nd 2020)

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #18

Patch file for stable/train (March 2nd 2020) (7.1 KiB, text/plain)

Patch file for stable/train (March 2nd 2020)

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #19

Patch file for stable/stein (March 2nd 2020) (6.3 KiB, text/plain)

Patch file for stable/stein (March 2nd 2020)

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #20

Patch file for stable/rocky (March 2nd 2020) (6.4 KiB, text/plain)

Patch file for stable/rocky (March 2nd 2020)

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #21

Patch file for stable/queens (March 2nd 2020) (6.4 KiB, text/plain)

Patch file for stable/queens (March 2nd 2020)

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #22

Patch file for stable/pike (March 2nd 2020) (6.5 KiB, text/plain)

Patch file for stable/pike (March 2nd 2020)

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-03: #23

Hello,

an update: patches have been refreshed for this bug, and attached here.

I reached out to Jeremy, and he agreed to take a look at this embargo
disclosure notice before I post it to <email address hidden> and <email
address hidden>. Thank you! Please let me know if i can change anything.
Next steps, after the draft message:

```
```

Subject: [pre-OSSA] Vulnerability in OpenStack Manila (CVE-2020-9543)

This is an advance warning of a vulnerability discovered in
OpenStack Manila, to give you, as downstream stakeholders, a chance to
coordinate the release of fixes and reduce the vulnerability window.
Please treat the following information as confidential until the
proposed public disclosure date.

OpenStack Manila <= 9.1.0 allows other project users to view, update,
delete, or share resources that do not belong to them, because of a
context-free lookup of a UUID. Attackers may also create resources, such
as shared file systems and groups of shares on such share networks.

Proposed patch:
See attached patches. Unless a flaw is discovered in them, these
patches will be merged to their corresponding branches on the public
disclosure date.

CVE: CVE-2020-9543

Proposed public disclosure date/time:
2020-03-09, 1500UTC
Please do not make the issue public (or release public patches)
before this coordinated embargo date.

Original private report:
https://bugs.launchpad.net/manila/+bug/1861485
For access to read and comment on this report, please reply to me
with your Launchpad username and I will subscribe you.

[...]

Attachments:
cve-2020-9543-master-ussuri.patch
cve-2020-9543-stable-train.patch
cve-2020-9543-stable-stein.patch
cve-2020-9543-stable-rocky.patch
cve-2020-9543-stable-queens.patch
cve-2020-9543-stable-pike.patch

```
```

Next Steps:

* On public disclosure (2020-03-09, 1500 UTC) - I'll switch this bug to
public, and coordinate with mnaser to upload the patches to
review.opendev.org.
* Tom and I will review/fast track approvals with the help of other cores
* Once patches have merged, I'll request a release from train, stein and
rocky branches. (The patches for queens and pike have only been provided
for courtesy - we will not perform a release on those branches).
* Simultaneously, I'll coordinate with the VMT team to publish an OSSA to
<email address hidden> and <email address hidden>.

Jeremy Stanley (fungi) wrote on 2020-03-03: #24

Goutham: your proposed pre-OSSA notification looks good. The VMT
recommends publishing advisories on Tuesdays, Wednesdays or Thursdays for
improved visibility, so you might consider moving your disclosure date to
Tuesday, March 10. Also be mindful that we're reaching EM status for
stable/rocky, so you may not want to commit to a Rocky point release, or
at least make sure up front that you're still going to be able to have one
next week.

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-04: #25

Thanks again, Jeremy. You're right regarding the rocky release, I'll drop
committing to that one since I know Sean/Elod wanted to get the release
out by 5th March [1]. I've asked, I'll wait out for any responses, and
revert here.

[1] http://lists.openstack.org/pipermail/openstack-discuss/2020-February/
012910.html

Goutham Pacha Ravi (gouthamr) wrote on 2020-03-10: #26

Switching this bug to "Public Security"

information type:Private Security → Public Security

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix proposed to manila (master)** #27

Fix proposed to branch: master
Review: https://review.opendev.org/712158

Changed in manila:
status:Confirmed → In Progress

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix proposed to manila (stable/train)** #28

Fix proposed to branch: stable/train
Review: https://review.opendev.org/712163

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix proposed to manila (stable/stein)** #29

Fix proposed to branch: stable/stein
Review: https://review.opendev.org/712164

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix proposed to manila (stable/rocky)** #30

Fix proposed to branch: stable/rocky
Review: https://review.opendev.org/712165

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix proposed to manila (stable/queens)** #31

Fix proposed to branch: stable/queens
Review: https://review.opendev.org/712166

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix proposed to manila (stable/pike)** #32

Fix proposed to branch: stable/pike
Review: https://review.opendev.org/712167

Goutham Pacha Ravi (gouthamr) on 2020-03-10

summary:- User knowing the id of a share network can show, delete, create share on
- a share network owned by different tenant
+ [OSSA-2020-002] Unprivileged users can retrieve, use and manipulate
+ share networks

Jeremy Stanley (fungi) on 2020-03-10

summary:[OSSA-2020-002] Unprivileged users can retrieve, use and manipulate
- share networks
+ share networks (CVE-2020-9543)

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix merged to manila (master)** #33

Reviewed: https://review.opendev.org/712158
Committed: https://git.openstack.org/cgit/openstack/manila/commit/?

id=947315f0903c823b0fdd9d99c60078814587272c
Submitter: Zuul
Branch: master

commit 947315f0903c823b0fdd9d99c60078814587272c
Author: Mohammed Naser <email address hidden>
Date: Fri Jan 31 16:13:24 2020 +0100

share_networks: enable project_only API only

At the moment, the share_network database API which the web
API layer interacts with directly does not have any checking
for project_id which means that a user has the ability to run
operations against any other share_network if they have the ID.

This patch implements the usage of project_only in the database
query which ensures that administrators still have the behaviour
of getting any share network they want, but users can only pull
up those which are part of their context/authenticated project.

This patch also adjusts a few other tests due to the fact that
the existing tests would run a lot of inserts with a different
project_id than the context, which is not allowed in this new
API behaviour. Therefore, the instances that involved projects
different than the context were converted to elevated ones.

There was also an instance where they were being created with a
project_id that did not match the fake context, therefore the
context was adjusted accordingly as well.

Closes-Bug: #1861485
Change-Id: Id67a939a475c4ac06d546b7e095bd10f1a6d2619

Changed in manila:
status:In Progress → Fix Released
tags:added: in-stable-train

OpenStack Infra (hudson-openstack) wrote on 2020-03-10: **Fix merged to manila (stable/train)** #34

Reviewed: https://review.opendev.org/712163
Committed: https://git.openstack.org/cgit/openstack/manila/commit/?id=496e6e1d2a074ab85f434fe2a88a6c0159696419
Submitter: Zuul
Branch: stable/train

commit 496e6e1d2a074ab85f434fe2a88a6c0159696419
Author: Mohammed Naser <email address hidden>
Date: Fri Jan 31 16:13:24 2020 +0100

share_networks: enable project_only API only

At the moment, the share_network database API which the web
API layer interacts with directly does not have any checking
for project_id which means that a user has the ability to run
operations against any other share_network if they have the ID.

This patch implements the usage of project_only in the database
query which ensures that administrators still have the behaviour
of getting any share network they want, but users can only pull
up those which are part of their context/authenticated project.

This patch also adjusts a few other tests due to the fact that
the existing tests would run a lot of inserts with a different
project_id than the context, which is not allowed in this new
API behaviour. Therefore, the instances that involved projects
different than the context were converted to elevated ones.

There was also an instance where they were being created with a
project_id that did not match the fake context, therefore the
context was adjusted accordingly as well.

Closes-Bug: #1861485
Change-Id: Id67a939a475c4ac06d546b7e095bd10f1a6d2619
(cherry picked from commit 947315f0903c823b0fdd9d99c60078814587272c)

OpenStack Infra (hudson-openstack) wrote on 2020-03-11: **Fix merged to manila (stable/stein)** #35

Reviewed: https://review.opendev.org/712164
Committed: https://git.openstack.org/cgit/openstack/manila/commit/?id=17b29e2b50d41db13f29eae86437ef91f6432c8d
Submitter: Zuul
Branch: stable/stein

commit 17b29e2b50d41db13f29eae86437ef91f6432c8d
Author: Mohammed Naser <email address hidden>
Date: Fri Jan 31 16:13:24 2020 +0100

share_networks: enable project_only API only

At the moment, the share_network database API which the web
API layer interacts with directly does not have any checking
for project_id which means that a user has the ability to run
operations against any other share_network if they have the ID.

This patch implements the usage of project_only in the database
query which ensures that administrators still have the behaviour
of getting any share network they want, but users can only pull
up those which are part of their context/authenticated project.

This patch also adjusts a few other tests due to the fact that
the existing tests would run a lot of inserts with a different
project_id than the context, which is not allowed in this new
API behaviour. Therefore, the instances that involved projects
different than the context were converted to elevated ones.

There was also an instance where they were being created with a
project_id that did not match the fake context, therefore the
context was adjusted accordingly as well.

Closes-Bug: #1861485
Change-Id: Id67a939a475c4ac06d546b7e095bd10f1a6d2619
(cherry picked from commit 947315f0903c823b0fdd9d99c60078814587272c)
(cherry picked from commit 496e6e1d2a074ab85f434fe2a88a6c0159696419)

tags:added: in-stable-stein

OpenStack Infra (hudson-openstack) wrote on 2020-03-11: **Fix merged to manila (stable/queens)** #36

```
Reviewed: https://review.opendev.org/712166
Committed: https://git.openstack.org/cgit/openstack/manila/commit/?
id=cf4963c5918572fe2d415d6268f5c746546cfada
Submitter: Zuul
Branch: stable/queens

commit cf4963c5918572fe2d415d6268f5c746546cfada
Author: Mohammed Naser <email address hidden>
Date: Fri Jan 31 16:13:24 2020 +0100

    share_networks: enable project_only API only

    At the moment, the share_network database API which the web
    API layer interacts with directly does not have any checking
    for project_id which means that a user has the ability to run
    operations against any other share_network if they have the ID.

    This patch implements the usage of project_only in the database
    query which ensures that administrators still have the behaviour
    of getting any share network they want, but users can only pull
    up those which are part of their context/authenticated project.

    This patch also adjusts a few other tests due to the fact that
    the existing tests would run a lot of inserts with a different
    project_id than the context, which is not allowed in this new
    API behaviour. Therefore, the instances that involved projects
    different than the context were converted to elevated ones.

    There was also an instance where they were being created with a
    project_id that did not match the fake context, therefore the
    context was adjusted accordingly as well.

    Closes-Bug: #1861485
    Change-Id: Id67a939a475c4ac06d546b7e095bd10f1a6d2619
    (cherry picked from commit 947315f0903c823b0fdd9d99c60078814587272c)
    (cherry picked from commit 496e6e1d2a074ab85f434fe2a88a6c0159696419)
    (cherry picked from commit 17b29e2b50d41db13f29eae86437ef91f6432c8d)
    (cherry picked from commit d16b5f0ea41419bdf4eb4e66ce4551571ee6acec)
    Signed-off-by: Goutham Pacha Ravi <email address hidden>

tags:added: in-stable-queens
```

OpenStack Infra (hudson-openstack) wrote on 2020-03-11: **Fix merged to manila (stable/rocky)** #37

```
Reviewed: https://review.opendev.org/712165
Committed: https://git.openstack.org/cgit/openstack/manila/commit/?
id=d16b5f0ea41419bdf4eb4e66ce4551571ee6acec
Submitter: Zuul
Branch: stable/rocky

commit d16b5f0ea41419bdf4eb4e66ce4551571ee6acec
Author: Mohammed Naser <email address hidden>
Date: Fri Jan 31 16:13:24 2020 +0100

    share_networks: enable project_only API only

    At the moment, the share_network database API which the web
    API layer interacts with directly does not have any checking
    for project_id which means that a user has the ability to run
    operations against any other share_network if they have the ID.

    This patch implements the usage of project_only in the database
    query which ensures that administrators still have the behaviour
    of getting any share network they want, but users can only pull
    up those which are part of their context/authenticated project.

    This patch also adjusts a few other tests due to the fact that
    the existing tests would run a lot of inserts with a different
    project_id than the context, which is not allowed in this new
    API behaviour. Therefore, the instances that involved projects
    different than the context were converted to elevated ones.

    There was also an instance where they were being created with a
    project_id that did not match the fake context, therefore the
    context was adjusted accordingly as well.

    Closes-Bug: #1861485
    Change-Id: Id67a939a475c4ac06d546b7e095bd10f1a6d2619
    (cherry picked from commit 947315f0903c823b0fdd9d99c60078814587272c)
    (cherry picked from commit 496e6e1d2a074ab85f434fe2a88a6c0159696419)
    (cherry picked from commit 17b29e2b50d41db13f29eae86437ef91f6432c8d)
    Signed-off-by: Goutham Pacha Ravi <email address hidden>

tags:added: in-stable-rocky
```

OpenStack Infra (hudson-openstack) wrote on 2020-03-12: **Fix merged to manila (stable/pike)** #38

```
Reviewed: https://review.opendev.org/712167
Committed: https://git.openstack.org/cgit/openstack/manila/commit/?
id=87799bbb13d7fa26bafefd16947216810183bb3b
Submitter: Zuul
Branch: stable/pike

commit 87799bbb13d7fa26bafefd16947216810183bb3b
Author: Mohammed Naser <email address hidden>
Date: Fri Jan 31 16:13:24 2020 +0100

    share_networks: enable project_only API only

    At the moment, the share_network database API which the web
    API layer interacts with directly does not have any checking
    for project_id which means that a user has the ability to run
    operations against any other share_network if they have the ID.

    This patch implements the usage of project_only in the database
    query which ensures that administrators still have the behaviour
    of getting any share network they want, but users can only pull
    up those which are part of their context/authenticated project.

    This patch also adjusts a few other tests due to the fact that
    the existing tests would run a lot of inserts with a different
    project_id than the context, which is not allowed in this new
```

```
    API behaviour. Therefore, the instances that involved projects
    different than the context were converted to elevated ones.

    There was also an instance where they were being created with a
    project_id that did not match the fake context, therefore the
    context was adjusted accordingly as well.

    Closes-Bug: #1861485
    Change-Id: Id67a939a475c4ac06d546b7e095bd10f1a6d2619
    (cherry picked from commit 947315f0903c823b0fdd9d99c60078814587272c)
    (cherry picked from commit 496e6e1d2a074ab85f434fe2a88a6c0159696419)
    (cherry picked from commit 039ab2b020e4ca13fa723b6cb931f921944894ee)
    (cherry picked from commit 496bb1473ea1ad8143bfb65d1727166de543affc)
    (cherry picked from commit c3b92b030aa3c0eda2549947df9b752c7393849e)
    Signed-off-by: Goutham Pacha Ravi <email address hidden>
```

tags:added: in-stable-pike

OpenStack Infra (hudson-openstack) wrote on 2020-03-12: **Fix included in openstack/manila 7.4.1** #39

```
This issue was fixed in the openstack/manila 7.4.1 release.
```

OpenStack Infra (hudson-openstack) wrote on 2020-03-26: **Fix included in openstack/manila 9.1.1** #40

```
This issue was fixed in the openstack/manila 9.1.1 release.
```

OpenStack Infra (hudson-openstack) wrote on 2020-03-26: **Fix included in openstack/manila 8.1.1** #41

```
This issue was fixed in the openstack/manila 8.1.1 release.
```

OpenStack Infra (hudson-openstack) wrote on 2021-07-29: **Fix included in openstack/manila queens-eol** #42

```
This issue was fixed in the openstack/manila queens-eol release.
```

See full activity log

To post a comment you must log in.