Log in / Register

OpenStack Dashboard (Horizon)

Overview Code Bugs Blueprints Translations Answers

[OSSA-2020-008] Open redirect in workflow forms (CVE-2020-29565)

Bug #1865026 reported by Radomir Dopieralski on 2020-02-27

This bug affects 2 people 270

Affects	Status	Importance	Assigned to	Milestone
OpenStack Dashboard (Horizon)	Fix Released	Undecided	Radomir Dopieralski	
OpenStack Security Advisory	Fix Released	Medium	Gage Hugo	

Bug Description

```
This affects all released versions of Horizon.

It is possible to make Horizon redirect to an arbitrary URL:

Steps of Reproduction:
1. Visit https://rhos-d.infra.prod.upshift.rdu2.redhat.com
2. Click on Instances
3. Pick any available instance and click on it.
4. On Right side - Click on Down arrow button
5. Hover on 'Edit Instance' and copy its link location and open in the
same browser in the same tab.
6. It will look like:
https://rhos-d.infra.prod.upshift.rdu2.redhat.com/dashboard/project/
instances/<instance_id>/update?step=instance_info&next=<path_and_id>;
Change the &next= value with &next=https://evil.com and refresh the page ;
then click on Save Button.
7. It will redirect the page to Evil.com.
```

Tags: in-stable-stein in-stable-train in-stable-ussuri

CVE References

2020-29565

Radomir Dopieralski (deshipu) wrote on 2020-02-27: #1

```
It looks like we have no validation on the "next" parameter, that is
getting passed to the target attribute of the form.

A possible fix could look like this:

diff --git a/horizon/workflows/views.py b/horizon/workflows/views.py
index 9c8fe1a27..2caf969e3 100644
--- a/horizon/workflows/views.py
+++ b/horizon/workflows/views.py
@@ -90,8 +90,14 @@ class WorkflowView(hz_views.ModalBackdropMixin,
generic.TemplateView):
         workflow = self.get_workflow()
         workflow.verify_integrity()
         context[self.context_object_name] = workflow
- next = self.request.GET.get(workflow.redirect_param_name)
- context['REDIRECT_URL'] = next
+ redirect_to = self.request.GET.get(workflow.redirect_param_name)
+ # Make sure the requested redirect matches the protocol,
+ # domain, and port of this request
+ if redirect_to and not http.same_origin(
+ request.build_absolute_uri(redirect_to),
+ request.build_absolute_uri()):
+ redirect_to = None
+ context['REDIRECT_URL'] = redirect_to
         context['layout'] = self.get_layout()
         # For consistency with Workflow class
         context['modal'] = 'modal' in context['layout']
```

Radomir Dopieralski (deshipu) wrote on 2020-02-27: #2

Suggested solution. (1.0 KiB, text/plain)

Jeremy Stanley (fungi) wrote on 2020-02-27: #3

```
Since this report concerns a possible security risk, an incomplete
security advisory task has been added while the core security
reviewers for the affected project or projects confirm the bug and
discuss the scope of any vulnerability along with potential
solutions.

description:updated
Changed in ossa:
     status:New → Incomplete
```

Jeremy Stanley (fungi) wrote on 2020-02-27: #4

```
It's not clear to me how an attacker would alter the "next" GET variable's
value supplied by Horizon. Can you elaborate on an actual exploit scenario
making use of this trick?
```

Jeremy Stanley (fungi) wrote on 2020-02-27: #5

```
Is the concern that someone might name, say, a server instance as that URL
and it will be passed through unaltered similar to bug 1247675? Or is the
concern simply that someone may send a maliciously-crafted Horizon URL to
someone out of band and socially engineer them into clicking on it? If the
latter, I think this may be a duplicate of (still private) bug 1825549.

Horizon security reviewers, can you take a look?
```

Report a bug

This report contains **Public Security** information

Everyone can see this security related information.

Duplicates of this bug

Bug #1825549

You are not directly subscribed to this bug's notifications.

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

Horizon Core secu...
Radomir Dopieralski
Summer Long

May be notified

ANish
Ahmed
Ahmed Ezzat
Aishwarya
Ajay Kumar
Akihiro Motoki
Alex Baretto
Alex Ermolov
Alfredzo Nash
Ali hussnain
Alistair Tonner
Andy Chong
Anna
Anten Skrabec
Anthony Young
April Wang
Arpita Rathi
Aruna Kushwaha
Asghar Riahi
Ashish Chandra
Ashish Kumar Singh
Ashokkumar c
Barki Mustapha
Branko Vukmirovic
Bruce Martins
C Sasi Kanth
Calub Viem
Cara O'Brien
Chris Samson
Christian Berendt
Christoph Fiehe
Craig Miller
David Cusatis
David Grizzanti
David Lapsley
David Lyle
David M. Zendzian
David Seelbach
Declan McGrath
Deepak Nair
DengBO
Devin Carlen
Dibyendu
Dongwon Cho
Douglas Mendizábal
Dustin Lundquist
Floren
Gage Hugo
Geronimo Orozco
Greg Althaus
Haobo Liu
Hosam Al Ali
Hugo Kou
Ian Y. Choi
Ivan Groenewald
Jamal Mitchell
Jared R Greene
Jay Janardhan
Jeff Ward
Jie Li

Radomir Dopieralski (deshipu) wrote on 2020-02-27: #6

As the value is automatically escaped when inserted into the template, the first scenario is not a concern.

The second scenario is a possibility, and is especially bad, as the request that reaches the malicious server is a POST request, containing all the data from the particular form (which, depending on which workflow is chosen, may contain sensitive data).

There is also another scenario, where this vulnerability is used together with some other vulnerability, like an XSS attack, to circumvent the same-origin restrictions and send harvested data embedded in the next URL to outside server.

I don't have access to bug 1825549 so I can't comment on that.

Jeremy Stanley (fungi) on 2020-05-19

description:updated

Jeremy Stanley (fungi) wrote on 2020-05-27: #7

The embargo for this report has expired and is now lifted, so it's acceptable to discuss further in public.

description:updated
information type:Private Security → Public Security

Radomir Dopieralski (deshipu) wrote on 2020-09-07: #8

Is there any update on this?

OpenStack Infra (hudson-openstack) on 2020-09-07

Changed in horizon:
assignee:nobody → Radomir Dopieralski (deshipu)
status:New → In Progress

OpenStack Infra (hudson-openstack) wrote on 2020-09-18: **Fix merged to horizon (master)** #9

```
Reviewed: https://review.opendev.org/750207
Committed: https://git.openstack.org/cgit/openstack/horizon/commit/?id=252467100f75587e18df9c43ed5802ee8f0017fa
Submitter: Zuul
Branch: master

commit 252467100f75587e18df9c43ed5802ee8f0017fa
Author: Radomir Dopieralski <email address hidden>
Date: Mon Sep 7 21:03:36 2020 +0200

    Fix open redirect

    Make sure the "next" URL is in the same origin as Horizon before
    redirecting to it.

    Change-Id: I06b2bfc8e3638591615547780c3fa34b0abe19f6
    Closes-bug: #1865026
```

Changed in horizon:
status:In Progress → Fix Released

OpenStack Infra (hudson-openstack) wrote on 2020-09-18: **Fix proposed to horizon (stable/ussuri)** #10

Fix proposed to branch: stable/ussuri
Review: https://review.opendev.org/752703

Jeremy Stanley (fungi) wrote on 2020-09-18: **Re: Open redirect in workflow forms** #11

Reviewing this and bug 1825549 they are both about lack of validation for the supplied value of the "next" parameter, so probably duplicates. I had classed the other report as merely security hardening, since the reporter apparently did not realize you could directly supply a URL there in some pages and get it to automatically redirect.

This sounds like a classic "CWE-601: URL Redirection to Untrusted Site ('Open Redirect')" (https://cwe.mitre.org/data/definitions/601.html) so probably a class A vulnerability report per https://security.openstack.org/vmt-process.html#incident-report-taxonomy if it can be cleanly patched on all affected stable branches.

OpenStack Infra (hudson-openstack) wrote on 2020-10-08: **Fix merged to horizon (stable/ussuri)** #12

```
Reviewed: https://review.opendev.org/752703
Committed: https://git.openstack.org/cgit/openstack/horizon/commit/?id=baa370f84332ad41502daea29a551705696f4421
Submitter: Zuul
Branch: stable/ussuri

commit baa370f84332ad41502daea29a551705696f4421
Author: Radomir Dopieralski <email address hidden>
Date: Mon Sep 7 21:03:36 2020 +0200

    Fix open redirect

    Make sure the "next" URL is in the same origin as Horizon before
    redirecting to it.

    Change-Id: I06b2bfc8e3638591615547780c3fa34b0abe19f6
    Closes-bug: #1865026
    (cherry picked from commit 252467100f75587e18df9c43ed5802ee8f0017fa)
```

tags:added: in-stable-ussuri

Joel wineland
John
John Lenihan
John Masciantoni
Jonas
Jordan Rinke
Joshua Padman
Kausal Malladi
Kausum Kumar
Ken'ichi Ohmichi
Kenji Motohashi
Kent Liu
Kun Huang
Kunal.Yadav
LIU Yulong
Le Tian Ren
Lei Zhang
LiuNanke
Louis Fourie
Lukas Koenen
Madhu CR
Mamta Jha
Manoj Raju
Marcos Lobo
Marcus Vinicius G...
Mark T. Voelker
Masco
Matthew Thode
MehdiAmirirad
Mehmet Hacısalihoğlu
Michael Rowland H...
Mika Kohonen
Mohan Seri
Mohankumar
Naved Ali
Naved Ali Shah
OpenStack Vulnera...
Pan Wei
Pankaj Mishra
Paul Voccio
Pavani_addanki
Perry Waldner
Pradeep Roy Kandru
Prateek
Prathyusha Vanka
Prosunjit Biswas
Rafi Khardalian
Rajesh Battala
Raju Alluri
Ranjit Ray
Richa
Rick Melick
Ritesh Khadgaray
Rochelle Grober
Ron Cannella
Ryo Shi
Satyanarayana Pat...
Sebastian Luna-Va...
Serena Chechile D...
Shades
Shawn Hartsock
Shruthi Chari
Sid Sun
Songhee Kang
Soo Choi
Steve Sloka
Steven Pavlon
Stuart Hart
Swaroop Jayanthi
Takashi Kajinami
Tao Zhou
Taurus Cheung
Tayaa Med Amine
Thongth
Tiago Everton Fer...
Toshiyuki Hayashi
Tushar Patil
Uma
Vidhisha Nair
Vinu Pillai
Vishal Manchanda
Vivek Agrawal
Wu Hong Guang
Xiang Hui
Xin Zhong
Yahoo! Engineerin...
Yash Bathia
Yongqiang Yang
Zahid Hasan
ZhangNi

Jeremy Stanley (fungi) wrote on 2020-10-08: **Re: Open redirect in workflow forms** #13

Once backports are in review for all of Horizon's supported stable branches, I'll proceed with requesting a CVE assignment and issuing an advisory.

Akihiro Motoki (amotoki) wrote on 2020-10-18: #14

Jeremy, what stable branches are in question? Is it enough to backport the patch to all branches in the maintained phase in https://releases.openstack.org/? Or Should we include "extended maintenance" branches?

Jeremy Stanley (fungi) wrote on 2020-10-18: #15

Yes, that's what we attempt to convey at https://security.openstack.org/vmt-process.html#supported-versions but I'll push an update for that text to use current release team terminology and link to the releases site.

Once backports are in review for all affected stable branches which are in a Maintained state per the table on the main page of the releases site, we can issue an advisory. If someone also wants to add patches for branches which are under Extended Maintenance then those can be included in the advisory as a convenience, but they are not required for us to be able to move forward with it.

OpenStack Infra (hudson-openstack) wrote on 2020-10-19: **Fix proposed to horizon (stable/train)** #16

Fix proposed to branch: stable/train
Review: https://review.opendev.org/758841

OpenStack Infra (hudson-openstack) wrote on 2020-10-19: **Fix proposed to horizon (stable/stein)** #17

Fix proposed to branch: stable/stein
Review: https://review.opendev.org/758843

Akihiro Motoki (amotoki) wrote on 2020-10-19: **Re: Open redirect in workflow forms** #18

Thanks Jeremy for the clarification.
I just pushed backports to all stable branches in the "maintained" phase.
(Regarding more backports to EM branches, I will discuss with other horizon stable cores.)

Gage Hugo (gagehugo) wrote on 2020-10-19: #19

First impact draft below, please review and suggest changes where needed.

@Radomir Dopieralski is there any organization/company you are affiliated with?

Title: Open redirect possible in Horizon workflow forms
Reporter: Radomir Dopieralski ()
Products: Horizon
Affects: <18.6.0, <18.3.2, <=16.2.0, <=15.3.1

Description:
Radomir Dopieralski () reported a vulnerability in Horizon's workflow forms. Previously there was a lack of validation on the "next" parameter, which would allow someone to supply a malicious URL in Horizon that can cause an automatic redirect to the provided malicious URL.

Summer Long (slong-g) wrote on 2020-10-20: #20

Hi Gage, do you have a CVE# from Mitre for this? Also, Radomir is Red Hat and raised this bug on behalf of a report by Pritam Singh <email address hidden>. thanks, Summer

Gage Hugo (gagehugo) wrote on 2020-10-20: #21

Not yet, once this draft is approved by the maintainers, I will request a CVE#.

Updated, please review:

Title: Open redirect possible in Horizon workflow forms
Reporter: Pritam Singh (Red Hat)
Products: Horizon
Affects: <18.6.0, <18.3.2, <=16.2.0, <=15.3.1

Description:
Pritam Singh (Red Hat) reported a vulnerability in Horizon's workflow forms. Previously there was a lack of validation on the "next" parameter, which would allow someone to supply a malicious URL in Horizon that can cause an automatic redirect to the provided malicious URL.

Gage Hugo (gagehugo) wrote on 2020-10-21: #22

Updated, please review:

Title: Open redirect possible in Horizon workflow forms
Reporter: Pritam Singh (Red Hat)
Products: Horizon
Affects: >=18.4.0 <18.6.0, >=17.0.0 <18.3.2, <=16.2.0, <=15.3.1

Description:
Pritam Singh (Red Hat) reported a vulnerability in Horizon's workflow forms. Previously there was a lack of validation on the "next" parameter, which would allow someone to supply a malicious URL in Horizon that can cause an automatic redirect to the provided malicious URL.

Jeremy Stanley (fungi) wrote on 2020-10-23: #23

Ziv
Ziyu Bai
ammarun
armyman420
avinashsau
brightson
bugtracker@devshe...
chaiwat wannaposop
chitu
congge
deepali verneya
devin.li
fei Yang
galeido
gsccc
iopenstack
jeff wang
kalim khuang
kgrvamsi
koolhead17
lanpi
laoyi
liaonanhai
lololmarwa255
longxingmiao
lpmqtt
maestropandy
malyadri
manish
manoj subramaniam
mershard frierson
miralaunchpad
mohit.048
nawawit kes
pawnesh kumar
pengyuesheng
raja
satyanarayana pat...
satyanarayana pat...
siva
sivagnanam C
tangfeixiong
truijllo
vivek.ys
wanghuagong
wenx999
xiaoningli
xreuze
yangbo
yangzhenyu
yongxiangwang
zhengyue

Patches

Suggested solution.

Add patch

Gage's impact description in comment #22 looks good to me, except for some slight adjustments to the affected versions line. We typically list affected versions from oldest to newest, and do a strictly less than (<) the next possible point release version for the branch, using an inclusive greater than or equal (>=) to indicate the start of any new ranges of affected releases, with commas (,) separating distinct ranges. The goal is that the resulting list of ranges remains correct after publication without us needing to know what the upcoming version numbers will necessarily be.

In this case, since the master branch fix merged before the Victoria release (leaving stable/victoria unaffected), the stable/ussuri backport merged but has not been tagged with a point release yet, and the remaining backports for stable/train and stable/stein are still under review, I would recommend the following series of affected version ranges:

```
    "<15.3.2, >=16.0.0 <16.2.1, >=17.0.0 <18.3.3"
```

This effectively means that we consider any tagged versions lower than 15.3.2 affected (no tag for this exists but it is the next lowest possible release number for the stable/stein branch). Similarly the 16.0.0 release and any subsequent releases less than 16.2.1 are affected (there is no 16.2.1 on stable/train and may never be, but any version numbers defined by that range are affected). Similarly for the stable/ussuri versions starting from 17.0.0 and less than 18.3.3 (next lowest possible point release on that branch).

OpenStack Infra (hudson-openstack) wrote on 2020-10-28: **Fix merged to horizon (stable/train)** #24

```
Reviewed: https://review.opendev.org/758841
Committed: https://git.openstack.org/cgit/openstack/horizon/commit/?
id=6c208edf323ced07b15ec4bc3879bddb91d398bc
Submitter: Zuul
Branch: stable/train

commit 6c208edf323ced07b15ec4bc3879bddb91d398bc
Author: Radomir Dopieralski <email address hidden>
Date: Mon Sep 7 21:03:36 2020 +0200

    Fix open redirect

    Make sure the "next" URL is in the same origin as Horizon before
    redirecting to it.

    Conflicts:
            horizon/test/unit/workflows/test_workflows.py

    Change-Id: I06b2bfc8e3638591615547780c3fa34b0abe19f6
    Closes-bug: #1865026
    (cherry picked from commit 252467100f75587e18df9c43ed5802ee8f0017fa)
    (cherry picked from commit baa370f84332ad41502daea29a551705696f4421)
```

tags:added: in-stable-train
tags:added: in-stable-stein

OpenStack Infra (hudson-openstack) wrote on 2020-10-28: **Fix merged to horizon (stable/stein)** #25

```
Reviewed: https://review.opendev.org/758843
Committed: https://git.openstack.org/cgit/openstack/horizon/commit/?
id=9e0e333ab5277b6c396f602862ff90398cb0242b
Submitter: Zuul
Branch: stable/stein

commit 9e0e333ab5277b6c396f602862ff90398cb0242b
Author: Radomir Dopieralski <email address hidden>
Date: Mon Sep 7 21:03:36 2020 +0200

    Fix open redirect

    Make sure the "next" URL is in the same origin as Horizon before
    redirecting to it.

    Conflicts:
            horizon/test/unit/workflows/test_workflows.py

    Change-Id: I06b2bfc8e3638591615547780c3fa34b0abe19f6
    Closes-bug: #1865026
    (cherry picked from commit 252467100f75587e18df9c43ed5802ee8f0017fa)
    (cherry picked from commit baa370f84332ad41502daea29a551705696f4421)
    (cherry picked from commit 6c208edf323ced07b15ec4bc3879bddb91d398bc)
```

Nick Tait (nickthetait) wrote on 2020-12-03: **Re: Open redirect in workflow forms** #26

Any news on CVE assignment?

Jeremy Stanley (fungi) wrote on 2020-12-03: #27

Revisiting more recent release activity since comment #23, this is what the affects line should include now:

<15.3.2, >=16.0.0 <16.2.1, >=17.0.0 <18.3.3, >=18.4.0 <18.6.0

15.3.2 was tagged with the fix before stable/stein transitioned to extended maintenance and all versions prior to it are assumed to be affected.

The first stable/train tag is 16.0.0 and most recent is 16.2.0, and the fix there has not been released yet so the earliest tag it could appear in would be 16.2.1.

The first stable/ussuri tag is 17.0.0 and most recent is 18.3.2, and the fix there has not been released yet so the earliest tag it could appear in would be 18.3.3.

The first stable/victoria tag is 18.4.0 and the fix there appeared in 18.6.0.

Gage Hugo (gagehugo) wrote on 2020-12-03: #28

Updated, please review:

```
Title: Open redirect possible in Horizon workflow forms
Reporter: Pritam Singh (Red Hat)
Products: Horizon
Affects: <15.3.2, >=16.0.0 <16.2.1, >=17.0.0 <18.3.3, >=18.4.0 <18.6.0

Description:
Pritam Singh (Red Hat) reported a vulnerability in Horizon's workflow
forms. Previously there was a lack of validation on the "next" parameter,
which would allow someone to supply a malicious URL in Horizon that can
cause an automatic redirect to the provided malicious URL.
```

Jeremy Stanley (fungi) wrote on 2020-12-03: #29

```
Gage, your updated impact description in comment #28 looks great, thanks!
You should be able to base a CVE request on that and push up an OSSA
change with a CVE placeholder in the meantime.
```

Gage Hugo (gagehugo) wrote on 2020-12-05: #30

```
OSSA gerrit: https://review.opendev.org/c/openstack/ossa/+/765388

CVE is pending.
```

Summer Long (slong-g) wrote on 2020-12-06: #31

```
Looks like CVE-2020-29565 has been assigned to this issue:
https://nvd.nist.gov/vuln/detail/CVE-2020-29565
```

Gage Hugo (gagehugo) on 2020-12-07

```
summary:- Open redirect in workflow forms
        + Open redirect in workflow forms (CVE-2020-29565)
```

Jeremy Stanley (fungi) wrote on 2020-12-08: #32

```
OSSA-2020-008 has been published to relevant mailing lists and the https:/
/security.openstack.org/ site.

Changed in ossa:
  assignee:nobody → Gage Hugo (gagehugo)
    status:Incomplete → Fix Released
importance:Undecided → Medium
   summary:- Open redirect in workflow forms (CVE-2020-29565)
           + [OSSA-2020-008] Open redirect in workflow forms (CVE-2020-29565)
```

OpenStack Infra (hudson-openstack) wrote on 2021-02-04: **Fix included in openstack/horizon 16.2.1** #33

```
This issue was fixed in the openstack/horizon 16.2.1 release.
```

OpenStack Infra (hudson-openstack) wrote on 2021-02-16: **Fix included in openstack/horizon 18.3.3** #34

```
This issue was fixed in the openstack/horizon 18.3.3 release.
```

OpenStack Infra (hudson-openstack) wrote on 2021-06-25: **Fix included in openstack/horizon pike-eol** #35

```
This issue was fixed in the openstack/horizon pike-eol release.
```

OpenStack Infra (hudson-openstack) wrote on 2021-07-16: **Fix included in openstack/horizon queens-eol** #36

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

See full activity log

To post a comment you must log in.

© 2004-2022 Canonical Ltd. • Terms of use • Data privacy • Contact Launchpad Support • Blog • Careers • System status • 31c7876 (Get the code!)