



# OpenStack Security Advisory

[Overview](#) [Code](#) [Bugs](#) [Blueprints](#) [Translations](#) [Answers](#)

## Compute service fails to restart if the vnic\_type of a bound port changed from direct to macvtap (CVE-2022-37394)

Bug #1981813 reported by [Balazs Gibizer](#) on 2022-07-15

This bug affects 1 person

256

Affects	Status	Importance	Assigned to	Milestone
<a href="#">OpenStack Compute (nova)</a>	Fix Released	Undecided	<a href="#">Balazs Gibizer</a>	
<a href="#">OpenStack Security Advisory</a>	In Progress	Undecided	<a href="#">David Wilde</a>	

### Bug Description

We have a downstream bug report with the following reproduction steps:

- 1) create a neutron port with vnic\_type "direct"
- 2) create an instance with that port
- 3) after the instance is created successfully change the vnic\_type of the bound port from "direct" to "macvtap". This is accepted by Neutron
- 4) wait until the nova instance info caches is healed by the periodic task in nova-compute
- 5) restart the nova-compute service.

Actual behavior

-----  
The nova-compute service fails to start with PciDeviceNotFoundById exception pointing to the PCI address of the VF the port is bound to on the host.

Expected behavior

-----  
The nova-compute service should start up successfully.

```
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service Traceback (most recent call last):
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/pci/utils.py", line
167, in get_ifname_by_pci_address
```

[Report a bug](#)

This report contains  
**Public Security**  
information

Everyone can see this  
security related  
information.

You are [not directly](#)  
subscribed to this bug's  
notifications.

[Edit bug mail](#)

### Other bug subscribers

[Subscribe someone else](#)

Notified of all  
changes

[Balazs Gibizer](#)

May be notified

-  
[ANish](#)  
[Ahmed](#)  
[Ahmed Ezzat](#)  
[Aishwarya](#)  
[Alex Baretto](#)  
[Alex Ermolov](#)  
[Alex Meade](#)  
[Alex Xu](#)  
[Alfred Shen](#)  
[Alfredzo Nash](#)  
[Ali hussnain](#)  
[Amir Sadoughi](#)  
[Andrea Frittoli](#)  
[Andrea Rosa](#)

```
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service dev_info = os.listdir(dev_path)
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service FileNotFoundError: [Errno 2] No such file or
directory: '/sys/bus/pci/devices/0000:19:0a.7/net'
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service During handling of the above exception, another
exception occurred:
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service Traceback (most recent call last):
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/usr/local/lib/python3.10/site-packages/
oslo_service/service.py", line 806, in run_service
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service service.start()
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/service.py", line
159, in start
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service self.manager.init_host()
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/compute/manager.py",
line 1536, in init_host
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service self._init_instance(context, instance)
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/compute/manager.py",
line 1230, in _init_instance
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service self.driver.plugin_vifs(instance, net_info)
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/virt/libvirt/driver.
py", line 1386, in plugin_vifs
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service self.vif_driver.plugin(instance, vif)
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/virt/libvirt/vif.py"
, line 730, in plugin
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service self.plugin_hw_vif(instance, vif)
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/virt/libvirt/vif.py"
, line 628, in plugin_hw_vif
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service set_vf_interface_vlan(
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/virt/libvirt/vif.py"
, line 99, in set_vf_interface_vlan
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service vf_ifname = pci_utils.get_ifname_by_pci_
```

[Andy Southgate](#)  
[Anna](#)  
[Anthony Young](#)  
[Antony Francis Ma...](#)  
[April Wang](#)  
[Arpita Rath](#)  
[Aruna Kushwaha](#)  
[Asghar Riahi](#)  
[Ashish Kumar Singh](#)  
[Augustina Ragwitz](#)  
[Aynur](#)  
[Barki Mustapha](#)  
[Bartlomiej Plotka](#)  
[Belmiro Moreira](#)  
[Bill Dymek](#)  
[Branko Vukmirovic](#)  
[Branko Vukmirovic](#)  
[Brian Wang](#)  
[Brin Zhang](#)  
[Bruce Basil Mathews](#)  
[Bruce Martins](#)  
[C Sasi Kanth](#)  
[Calub Viem](#)  
[Cara O'Brien](#)  
[Chason Chan](#)  
[Chinmay Naik](#)  
[Chris Samson](#)  
[Christian Berendt](#)  
[Christoph Fiehe](#)  
[Craig Miller](#)  
[David Lapsley](#)  
[David M. Zendzian](#)  
[David Pravec](#)  
[David Seelbach](#)  
[David Wilde](#)  
[Deepak Nair](#)  
[DengBO](#)  
[Derek Ragona](#)  
[Devdeep Singh](#)  
[Donghoon Kim](#)  
[Dongwon Cho](#)  
[Douglas Mendizábal](#)  
[Dustin Lundquist](#)  
[Ed Villalovoz](#)  
[Eric Kwon](#)

```

address(pci_addr)
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service File "/opt/stack/nova/nova/pci/utils.py", line
170, in get_ifname_by_pci_address
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service raise exception.PciDeviceNotFoundById(id=pci_
addr)
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service nova.exception.PciDeviceNotFoundById: PCI
device 0000:19:0a.7 not found
Jul 15 06:39:14 dell-r640-020 nova-compute[278453]: ERROR
oslo_service.service

```

Tags: [compute](#) [neutron](#) [pci](#)

## CVE References

[2022-37394](#)

Balazs Gibizer (balazs-gibizer) on 2022-07-15	
<p>Changed in nova:</p> <p><b>assignee:</b>nobody → Balazs Gibizer (balazs-gibizer)</p> <p><b>tags:</b>added: neutron pci</p> <p><b>tags:</b>added: compute</p>	
OpenStack Infra (hudson-openstack) wrote on 2022-07-15: <b>Related fix proposed to nova (master)</b>	#1
<p>Related fix proposed to branch: master</p> <p>Review: <a href="https://review.opendev.org/c/openstack/nova/+849985">https://review.opendev.org/c/openstack/nova/+849985</a></p>	
OpenStack Infra (hudson-openstack) wrote on 2022-07-15: <b>Fix proposed to nova (master)</b>	#2
<p>Fix proposed to branch: master</p> <p>Review: <a href="https://review.opendev.org/c/openstack/nova/+850003">https://review.opendev.org/c/openstack/nova/+850003</a></p> <p>Changed in nova:</p> <p><b>status:</b>New → In Progress</p>	
sean mooney (sean-k-mooney) on 2022-07-15	
<b>information type:</b> Public → Public Security	
Jeremy Stanley (fungi) wrote on 2022-07-15: <b>Re: Compute service fails to restart if the vnic_type of a bound port changed from direct to macvtap</b>	#3

[Eric Xie](#)  
[Fontenay Tony](#)  
[Gage Hugo](#)  
[Gaurav Singh](#)  
[Gavin B](#)  
[Greg Althaus](#)  
[Guangya Liu \(Jay ...](#)  
[Haobo Liu](#)  
[Haochen Zhang](#)  
[Harikrishna S](#)  
[Hohyun, Jeon](#)  
[Hohyun, Jeon](#)  
[Honorarac.Org](#)  
[Hosam Al Ali](#)  
[Hugo Kou](#)  
[Hui Cheng](#)  
[Ian Y. Choi](#)  
[Ilya Alekseyev](#)  
[Ivan Groenewald](#)  
[Jamal Mitchell](#)  
[Jared R Greene](#)  
[Jay Janardhan](#)  
[Jeff Ward](#)  
[Jia Dong](#)  
[Jie Li](#)  
[Jiyong Zhang](#)  
[Joel wineland](#)  
[John](#)  
[John Herndon](#)  
[John Lenihan](#)  
[John Masciantoni](#)  
[Jordan Rinke](#)  
[Joshua Padman](#)  
[Juergen Leopold](#)  
[Jung hyunjin](#)  
[Kausal Malladi](#)  
[Kausum Kumar](#)  
[Kei Masumoto](#)  
[Ken'ichi Ohmichi](#)  
[Kenji Motohashi](#)  
[Kent Liu](#)  
[Kunal.Yadav](#)  
[LIU Yulong](#)  
[Lawrnecy Meng](#)  
[Le Tian Ren](#)

Sean: Can you elaborate on why you believe this report represents an exploitable security vulnerability? Is it that a malicious user can change the vnic\_type of a port under their control and leave a time-bomb for the next time the administrator restarts the compute service, resulting in that compute host being out of service (unable to stop/start running virtual machines) until the problem can be manually rectified?

Jeremy Stanley (fungi) wrote on 2022-07-18:

#4

I caught up with Sean in IRC and he confirmed the situation is basically as I inferred above (exploitable by any normal authenticated user, not just limited to operator level accounts).

Changed in ossa:

**status:**New → Incomplete

Jeremy Stanley (fungi) wrote on 2022-07-18:

#5

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.

David Wilde (dave-wilde) wrote on 2022-07-19:

#6

Title: Compute service fails to restart if the vnic\_type of a bound port changed from direct to macvtap  
Reporter: Balazs Gibizer (Red Hat)  
Products: Nova  
Affects: >=23.0.0  
  
Description:  
Balazs Gibizer with Red Hat reported a vulnerability in Nova's restart behavior when a Neutron port type is changed from "direct" to "macvtap". By creating a neutron port with vnic\_type "direct", creating an instance bound to that port, and then changing the vnic\_type of the bound port to "macvtap" an authenticated user may cause the compute service to fail to restart resulting in a possible denial of service.  
Only Nova deployments configured with SR-IOV are affected.

Balazs Gibizer (balazs-gibizer) wrote on 2022-07-19:

#7

@David: Your summary look good to me.  
@fungi: <https://review.opendev.org/c/openstack/nova/+850003> is proposed as a mitigation of the denial of service. With that patch nova will no longer fail to restart in the reported situation.

Lei Zhang  
Lewis Denny  
Li Xipeng  
Lisathomes  
Louis Fourie  
Lukas Koenen  
Madhu CR  
Mamta Jha  
Manikantha Sriniv...  
Manoj Raju  
Marcus Vinicius G...  
Mario Carvalho  
Mark McLoughlin  
Marta Sdvoijspa  
Matthew Thode  
Meera Belur  
Michael Rowland H...  
Mika Kohonen  
Mike Evenosky  
Milind Barve  
Mohankumar  
Nanda Kishore  
Naved Ali  
Naved Ali Shah  
Nayna Patel  
Normen Scholtke  
OpenStack Vulnera...  
Pankaj Mishra  
Paul Voccio  
Pavani\_addanki  
Perry Waldner  
Piet Delaney  
Piyana Saowaratt...  
Pradeep Roy Kandru  
Pranali Deore  
Prateek  
Prithiv Mohan  
Prosunjit Biswas  
Rafi Khardalian  
Rajesh Battala  
Raju Alluri  
Ranjit Ray  
Ratnaker  
RaviM Singh  
Ray Trejo

Jeremy Stanley (fungi) wrote on 2022-07-19:

#8

Thanks David!

Keep in mind that the title is what will appear in the list of advisories at <https://security.openstack.org/ossalist.html> and will be combined with the project name, OSSA number and CVE identifier in the subject line of advisories posted to widely-read public mailing lists, so shorter is better as long as it still uniquely captures the situation, sort of like a commit message title. Maybe something along the lines of "Changing vnic\_type breaks compute service restart" instead (50 characters).

For the affected versions, we assume that a fix will be backported to all stable series currently in a "managed" state (so Wallaby, Xena and Yoga in this case) and that stable point releases will be tagged to include those. Since the most recent point releases are 23.2.1, 24.1.1 and 25.0.1 we indicate that the next possible release number for each of these is not affected like so: <23.2.2, >=24.0.0 <24.1.2, >=25.0.0 <25.0.2 (if the next point release on stable/yoga ends up being 25.1.0 instead and there is never a 25.0.2 that's fine, since 25.1.0 still falls into an unaffected range strictly speaking).

David Wilde (dave-wilde) wrote on 2022-07-21:

#9

Thanks for the feedback Jeremy, especially the calculation for the point releases. That was confusing me but your explanation makes perfect sense. Here's my updated description:

Title: Changing vnic\_type breaks compute service restart

Reporter: Balazs Gibizer (Red Hat)

Products: Nova

Affects: <23.2.2, >=24.0.0 <24.1.2, >=25.0.0 <25.0.2

Description:

Balazs Gibizer with Red Hat reported a vulnerability in Nova's restart behavior when a Neutron port type is changed from "direct" to "macvtap". By creating a neutron port with vnic\_type "direct", creating an instance bound to that port, and then changing the vnic\_type of the bound port to "macvtap" an authenticated user may cause the compute service to fail to restart resulting in a possible denial of service.

Only Nova deployments configured with SR-IOV are affected.

Jeremy Stanley (fungi) wrote on 2022-07-21:

#10

David's proposed impact description from comment #9 looks perfect to me. If there are no immediate objections, VMT members can proceed in requesting a CVE assignment based on that description while the master branch fix is under review, and then work on assembling an advisory once backports have been pushed.

David Wilde (dave-wilde) on 2022-08-01

Richa

Rick Melick

Robert Carr

Rochelle Grober

Rohini Diwakar

Ron Cannella

Rongze Zhu

Ryo Shi

Salvatore Orlando

Sanjay Tripathi

Sateesh

Satya Sanjibani R...

Satyanarayana Pat...

Scott Sanchez

Sebastian Luna-Va...

Shawn Hartsock

Shruthi Chari

Sid Sun

Simon

Songhee Kang

Soo Choi

Spencer Yu

Sridhar Gaddam

Steve Sloka

Steven Pavlon

Steven Relf

Stuart Hart

Summer Long

Surya N

Surya Seetharaman

Sushma Korati

Swami Reddy

Swaroop Jayanthi

Takashi Kajinami

Tao Zhou

Taurus Cheung

Tayaa Med Amine

Thongth

Tiago Everton Fer...

Tushar Patil

Uma

Venkata Anil

Venkata Siva Vija...

Vidhisha Nair

Vilobh Meshram

Changed in ossa:

**status:**Incomplete → In Progress

**assignee:**nobody → David Wilde (dave-wilde)

**David Wilde (dave-wilde)** on 2022-08-03

**summary:**Compute service fails to restart if the vnic\_type of a bound port

- changed from direct to macvtap
- + changed from direct to macvtap (CVE-2022-37394)

**OpenStack Infra (hudson-openstack)** wrote on 2022-09-08: **Related fix merged to nova (master)**

#11

Reviewed: <https://review.opendev.org/c/openstack/nova/+849985>  
Committed: <https://opendev.org/openstack/nova/commit/f8c91eb75fc5504a37fc3b4be1d65d33dbc9b511>  
Submitter: "Zuul (22348)"  
Branch: master

commit f8c91eb75fc5504a37fc3b4be1d65d33dbc9b511  
Author: Balazs Gibizer <email address hidden>  
Date: Fri Jul 15 12:43:58 2022 +0200

Reproduce [bug 1981813](#) in func env

Related-Bug: #1981813  
Change-Id: I9367b7ed475917bdb05eb3f209ce1a4e646534e2

**OpenStack Infra (hudson-openstack)** wrote on 2022-09-10: **Fix merged to nova (master)**

#12

Reviewed: <https://review.opendev.org/c/openstack/nova/+850003>  
Committed: <https://opendev.org/openstack/nova/commit/e43bf900dc8ca66578603bed333c56b215b1876e>  
Submitter: "Zuul (22348)"  
Branch: master

commit e43bf900dc8ca66578603bed333c56b215b1876e  
Author: Balazs Gibizer <email address hidden>  
Date: Fri Jul 15 13:48:46 2022 +0200

Gracefully ERROR in \_init\_instance if vnic\_type changed

If the vnic\_type of a bound port changes from "direct" to "macvtap" and then the compute service is restarted then during \_init\_instance nova tries to plug the vif of the changed port. However as it now has macvtap vnic\_type nova tries to look up the netdev of the parent VF. Still that VF is consumed by the instance so there is no such netdev on the host

Vinu Pillai  
Vish Ishaya  
Vladik Romanovskiy  
Wayne A. Walls  
William Wolf  
WuBing  
Xiang Hui  
Xin Zhong  
Yahoo! Engineerin...  
Yalu Bai  
Yongqiang Yang  
You, Ji  
Yusuf Güngör  
Zahid Hasan  
ZhangNi  
Ziv  
aginwala  
ammarun  
armyman420  
avinashsau  
brightson  
bugtracker@devshe...  
chaiwat wannaposop  
chitu  
congge  
david  
dk647  
droom  
fei yang  
fhbeak60161  
galeido  
gsccc  
hougangliu  
iopenstack  
james kang  
jay.xu  
jeff wang  
kalim khuang  
kgrvamsi  
lanpi  
laoyi  
liaonanhai  
lica  
lin han  
liuwei

OS. This error killed the compute service at startup due to unhandled exception. This patch adds the exception handler, logs an ERROR and continue initializing other instances on the host.

Also this patch adds a detailed ERROR log when nova detects that the vnic\_type changed during \_heal\_instance\_info\_cache periodic.

Closes-Bug: #1981813  
Change-Id: I1719f8eda04e8d15a3b01f0612977164c4e55e85

Changed in nova:  
**status:**In Progress → Fix Released

OpenStack Infra (hudson-openstack) wrote on 2022-09-16: **Fix included in openstack/nova 26.0.0.0rc1**

#13

This issue was fixed in the openstack/nova 26.0.0.0rc1 release candidate.

OpenStack Infra (hudson-openstack) wrote on 2022-09-26: **Related fix proposed to nova (stable/yoga)**

#14

Related fix proposed to branch: stable/yoga  
Review: <https://review.opendev.org/c/openstack/nova/+859312>

OpenStack Infra (hudson-openstack) wrote on 2022-09-26: **Fix proposed to nova (stable/yoga)**

#15

Fix proposed to branch: stable/yoga  
Review: <https://review.opendev.org/c/openstack/nova/+859313>

OpenStack Infra (hudson-openstack) wrote on 2022-09-26: **Related fix proposed to nova (stable/xena)**

#16

Related fix proposed to branch: stable/xena  
Review: <https://review.opendev.org/c/openstack/nova/+859314>

OpenStack Infra (hudson-openstack) wrote on 2022-09-26: **Fix proposed to nova (stable/xena)**

#17

Fix proposed to branch: stable/xena  
Review: <https://review.opendev.org/c/openstack/nova/+859315>

OpenStack Infra (hudson-openstack) wrote on 2022-09-26: **Related fix proposed to nova (stable/wallaby)**

#18

liuzhuangzhuang  
lololmarwa255  
lpmqtt  
maestropandy  
manish  
melanie witt  
mershard frierson  
mimul  
miralaunchpad  
mohit.048  
nawawit kes  
neethi shashidhar  
phalgun sirga  
raja  
ramesram  
robin  
sangbaobao  
satyanarayana pat...  
satyanarayana pat...  
shadyabhi  
shiliang  
sivagnanam C  
soumiyajit  
sunilcn  
tangfeixiong  
victorye81  
vishwa  
vivek.js  
vks1  
wanghuagong  
wangqiang.sheng  
woody89  
xianliangchi  
xiaoningli  
xreuze  
ya.wang  
yangbo  
yangkai  
yangzhenyu  
yanxubin  
yilong  
yongxiangwang  
yysimida  
zhengyue  
zhu zhu

Related fix proposed to branch: stable/wallaby  
Review: <https://review.opendev.org/c/openstack/nova/+859320>

[zhuangkai.zong](#)

OpenStack Infra (hudson-openstack) wrote on 2022-09-26: **Fix proposed to nova (stable/wallaby)**

#19

Fix proposed to branch: stable/wallaby  
Review: <https://review.opendev.org/c/openstack/nova/+859321>

[See full activity log](#)

To post a comment you must [log in](#).

 Launchpad • [Take the tour](#) • [Read the guide](#)  

© 2004-2022 Canonical Ltd. • [Terms of use](#) • [Data privacy](#) • [Contact Launchpad Support](#) • [Blog](#) • [Careers](#) • [System status](#) • 34b419c ([Get the code!](#))