



[OSSA-2021-004] Linuxbridge ARP filter bypass on Netfilter platforms (CVE-2021-38598)

Bug #1938670 reported by [Jake Yip](#) on 2021-08-02

This bug affects 1 person

260

Affects	Status	Importance	Assigned to	Milestone
OpenStack Security Advisory	Fix Released	High	Jeremy Stanley	
neutron	Fix Released	Undecided	Rodolfo Alonso	

Bug Description

We are running an OpenStack cloud with linux bridge. We have found that, in certain conditions, ARP spoofing protection is not working as intended. This allows a user do bad things like spoof gratuitous ARP to DoS another user's virtual machine. More details below.

In an environment using linux bridge, neutron-linuxbridge-agent uses ebttables to prevent ARP spoofing. A list of typical ebttables rules for a VM looks like this:

```
:neutronMAC-tapdb545a8c-8f DROP
:neutronARP-tapdb545a8c-8f DROP
-A PREROUTING -i tapdb545a8c-8f -j neutronMAC-tapdb545a8c-8f
-A PREROUTING -p ARP -i tapdb545a8c-8f -j neutronARP-tapdb545a8c-8f
-A neutronMAC-tapdb545a8c-8f -i tapdb545a8c-8f --among-src
fa:16:3e:84:cd:b4 -j RETURN
-A neutronARP-tapdb545a8c-8f -p ARP --arp-ip-src 192.0.2.5 -j ACCEPT
```

The neutronARP-xxx chain, however, has a problem during the creation of it. The source for that [1] looks like this:

```
ebtables(['-N', vif_chain, '-P', 'DROP'])
ebtables(['-F', vif_chain])
```

This creates a chain with default policy of DROP, and FLUSHes any existing rules.

However, we have found that in certain OS, the FLUSH reverts the default policy back to RETURN. E.g.

```
root@jake-focal:~# eatables -t nat -N newchain -P DROP
root@jake-focal:~# ebttables-save | grep newchain
:newchain DROP
root@jake-focal:~# ebttables -t nat -F newchain
root@jake-focal:~# ebttables-save | grep newchain
:newchain RETURN
root@jake-focal:~# ebttables --version
ebtables 1.8.4 (nf_tables)
```

The OSes that exhibit this issue seems to be OSes that uses ebttables-nft - Ubuntu Focal, CentOS Stream.

Ubuntu Bionic is fine. E.g.

```
root@jake-bionic:~# ebttables -t nat -N newchain -P DROP
root@jake-bionic:~# ebttables-save | grep newchain
:newchain DROP
root@jake-bionic:~# ebttables -t nat -F newchain
root@jake-bionic:~# ebttables-save | grep newchain
:newchain DROP
root@jake-bionic:~# ebttables --version
ebtables v2.0.10-4 (December 2011)
```

I have a patch for this, but as this is a security issue I am refraining from posting it up to OpenStack's Gerrit. Also, this might have been fixed in master, but it still affects Ussuri and Victoria. Please advise on what I should do next?

[1] https://opendev.org/openstack/neutron/src/branch/stable/ussuri/neutron/plugins/ml2/drivers/linuxbridge/agent/arp_protect.py#L135-L139

[See original description](#)

Tags: [in-stable-train](#) [in-stable-ussuri](#) [in-stable-victoria](#)

CVE References

Jeremy Stanley (fungi) wrote on 2021-08-02:	#1
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. Changed in ossa: status:New → Incomplete description:updated	
Rodolfo Alonso (rodolfo-alonso-herandez) on 2021-08-10	
Changed in neutron: assignee:nobody → Rodolfo Alonso (rodolfo-alonso-herandez) status:New → Confirmed	
Rodolfo Alonso (rodolfo-alonso-herandez) wrote on 2021-08-10:	#2

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

[Jake Yip](#)
[Justin Mammarella](#)
[Neutron Core Secu...](#)

May be notified

[ANish](#)
[Abhiraj Butala](#)
[Abu Shohel Ahmed](#)
[Ahmed](#)
[Ahmed Ezzat](#)
[Aishwarya](#)
[Akihiro Motoki](#)
[Alex Baretto](#)
[Alex Ermolov](#)
[Alfredzo Nash](#)
[Ali Jabbar](#)
[Ali hussnain](#)
[Amir Sadoughi](#)
[Andrej](#)
[Andrew Boik](#)
[Angna Aggarwal](#)
[Ankur](#)
[Anna](#)
[April Wang](#)
[Armando Migliaccio](#)
[Arpita Rath](#)
[Arun Sharma](#)
[Aruna Kushwaha](#)
[Asghar Riahi](#)
[Ashish Kumar Singh](#)
[Ashok kumaran B](#)
[Atif](#)
[Aziz](#)
[Bao Fangyan](#)
[Barki Mustapha](#)
[Bathri Ajay Raj](#)
[Bernard Cafarelli](#)
[Brad Eckert](#)
[Branko Vukmirovic](#)
[Brian Bowen](#)
[Brian Haley](#)
[Brian Shang](#)
[Bruce Martins](#)
[C Sasi Kanth](#)
[Calub Viem](#)
[Canh Truong](#)
[Cara O'Brien](#)
[Chason Chan](#)
[Cheng Zuo](#)
[Chris Samson](#)
[Christoph Fiehe](#)
[Craig Miller](#)
[Dan Sneddon](#)
[Daniel Alvarez](#)
[Dave Cahill](#)
[David Lapsley](#)
[David M. Zendzian](#)
[David Seelbach](#)
[Davish Bhardwaj](#)
[Deepak Nair](#)
[DengBO](#)
[Dmitriy Andrushko](#)
[Dong Jun](#)
[Dongwon Cho](#)
[Douglas Mendizábal](#)
[Duc Nguyen](#)
[Dustin Lundquist](#)
[Edgar Magana](#)

Hello:

Thank you for the report. That was solved in master and W in [1]. This patch flushes or creates the related "vif_chain" and then adds a default DROP rule [2][3].

I'll backport this patch up to Queens. Although the patch description is not related to this one, it is indeed solving what is described.

Regards.

[1]<https://review.opendev.org/q/I9463b000f6f63e65aaf91d60b30f6c92c01e3baf>

[2]https://review.opendev.org/c/openstack/neutron/+785177/3/neutron/plugins/ml2/drivers/linuxbridge/agent/arp_protect.py#122

[3]https://review.opendev.org/c/openstack/neutron/+785177/3/neutron/plugins/ml2/drivers/linuxbridge/agent/arp_protect.py#128

Jeremy Stanley (fungi) wrote on 2021-08-10:

#3

Rodolfo: Thanks for working on this. Unfortunately when you pushed your backports today you linked to this private vulnerability report in the commit messages, breaking the embargo. As a result, I'm going ahead and switching the bug to Public Security status and proceeding under our public report workflow.

description:updated

information type:Private Security → Public Security

Jeremy Stanley (fungi) on 2021-08-10

Changed in ossa:

status:Incomplete → Confirmed

importance:Undecided → High

assignee:nobody → Jeremy Stanley (fungi)

Jeremy Stanley (fungi) wrote on 2021-08-10:

#4

We've been treating other unintended anti-spoofing filter bypasses as class A reports lately, most recently OSSA-2021-001 which had a similar impact and risks (though with differing details obviously), so I'll start putting together an impact description and we'll publish an advisory once the backports for stable/victoria and stable/ussuri merge.

Rodolfo Alonso (rodolfo-alonso-herandez) wrote on 2021-08-10:

#5

Hello Jeremy:

This is the first time I actually provide a patch for a bug with an embargo. Sorry for breaking it. Next time I'll be more careful.

Regards.

Jeremy Stanley (fungi) wrote on 2021-08-10:

#6

Rodolfo: Don't sweat it, the other anti-spoofing bypass vulnerability I mentioned was public for a very long time before it was fixed, and I was going to start a conversation about switching this to public ahead of publication anyway. We just prefer to have the opportunity to discuss that decision first if the report was originally provided in private.

For future reference though, when a report of a suspected vulnerability is still in Private Security status we keep a paragraph at the top of the bug description which includes reminders not to mention or link the report in public code review, mailing lists, IRC and so on (I removed it from this bug when switching it to Public Security, but you can find it in the full activity log). The hope is that developers will read that notice before taking further action.

Anyway, thanks for the fixes and for moving this along, I'll push up a draft advisory we can all review, and then file a CVE assignment request with that text once we're satisfied with the details in it.

OpenStack Infra (hudson-openstack) wrote on 2021-08-10: Fix proposed to ossa (master)

#7

Fix proposed to branch: master

Review: <https://review.opendev.org/c/openstack/ossa/+804116>

Changed in ossa:

status:Confirmed → In Progress

Jeremy Stanley (fungi) wrote on 2021-08-10: Re: linuxbridge: ebttables-nft allows ARP spoofing

#8

Please review the proposed advisory text and affected version ranges in <https://review.opendev.org/804116> and, if that looks correct, I'll apply to MITRE for a CVE using that description.

Jake: I've credited the discovery to "Jake Yip" and "Nectar" but please let me know if you'd like to go by a different name and/or list a different organizational affiliation (the university, maybe something else?). Thanks!

Jake Yip (waipengyip) wrote on 2021-08-10:

#9

Hi Jeremy,

Please credit it to

"Jake Yip from ARDC and Justin Mammarella from the University of Melbourne"

Thanks!

Jeremy Stanley (fungi) wrote on 2021-08-11:

#10

- Edward
- Elena Ezhova
- Elvira García Ruiz
- Euler Jiang
- Evgeny Fedoruk
- Flavio Fernandes
- Florin Vinti
- Fontenay Tony
- Gage Hugo
- Gandharva
- Ganesh Kadam
- Gary Kotton
- Greg Althaus
- Guangya Liu (Jay ...
- HENG ZHANG
- HaifengLi
- Hampapur Ajay
- Hao Wang
- Harikrishna S
- Harkirat Singh
- Harsh Prasad
- Hemant Jadhav
- Hemanth Ravi
- Hirofumi Ichihara
- Hong Hui Xiao
- Hosam Al Ali
- Hugo Kou
- Hui Cheng
- Ian Y. Choi
- Igor D.C.
- Ihar Hrachyshka
- Ivan Groenewald
- Jamal Mitchell
- James Denton
- Jared R Greene
- Jay Janardhan
- Jeff Ward
- Jeremy Stanley
- Jiajun Liu
- Jie Li
- Jinlai Shan
- Joel wineland
- John
- John Buswell
- John Davidge
- John Kasperski
- John Lenihan
- John Perkins
- Jordan Rinke
- Joshua Padman
- Kausal Malladi
- Kausum Kumar
- Ken'ichi Ohmichi
- Kenji Motohashi
- Kent Liu
- Kevin Benton
- Kunal.Yadav
- LIU Yulong
- Lajos Katona
- Le Tian Ren
- Lei Zhang
- Lewis Denny
- Li Xipeng
- Lionel Zerbib
- Louis Fourie
- Lujin Luo
- Lukas Koenen
- MARZAK Ilham
- Maciej Jozefczyk
- Madhu CR
- Mamatisa Nurmatov
- Mamta Jha
- Manikanta Srinivas
- Manikantha Sriniv...
- Manish Godara
- Manjeet Singh Bhatia
- Manoj Raju
- Marcus Vinicius G...
- Mark McClain
- Marta Sdvojspa
- Matthew Thode
- Michael Rowland H...
- Michael Tietz
- Michael Thompson
- Miguel Lavalle
- Mika Kohonen
- Mohankumar
- Mohit Malik
- Murali Raju
- Na Zhu

Jake: Thanks for the correction, I've updated it in the proposed advisory now as requested.

Jeremy Stanley (fungi) wrote on 2021-08-12:	#11
<p>I have requested a CVE through MITRE's form based on the summary in https://review.opendev.org/804116 and will update that proposed advisory, as well as this bug, with it once assigned.</p> <p>summary:- linuxbridge: ebttables-nft allows ARP spoofing + Linuxbridge ARP filter bypass on Netfilter platforms</p>	

Jeremy Stanley (fungi) on 2021-08-12
<p>summary:- Linuxbridge ARP filter bypass on Netfilter platforms + Linuxbridge ARP filter bypass on Netfilter platforms (CVE-2021-38598)</p>

OpenStack Infra (hudson-openstack) wrote on 2021-08-16: Fix merged to neutron (stable/victoria)	#12
<p>Reviewed: https://review.opendev.org/c/openstack/neutron/+804056 Committed: https://opendev.org/openstack/neutron/commit/fafa5dacd5057120562184a734e7345e7c0e9639 0562184a734e7345e7c0e9639 Submitter: "Zuul (22348)" Branch: stable/victoria</p> <p>commit fafa5dacd5057120562184a734e7345e7c0e9639 Author: Rodolfo Alonso Hernandez <email address hidden> Date: Wed Apr 7 13:16:21 2021 +0000</p> <p>Make ARP protection commands compatible with "ebtables-nft"</p> <p>"nftables" compatible binary, "ebtables-nft", is not 100% compatible with the legacy API, as reported in LP#1922892.</p> <p>This patch fixes the following issues when using "ebtables-nft" (while keeping compatibility with legacy binary):</p> <ul style="list-style-type: none">- When a new chain is created, a default DROP rule is added at the end of the chain (append). This will prevent the error code 4 when the chain is listed.- The chain rules are added at the begining of the chain (insert), before the default DROP rule. This will prioritize the port rules.- The MAC rules are cleaned before the new ones are added. That will prevent the deletion of any new needed rule, now added after the deletion.- The "ebtables" command will retry on error code 4. This is the error returned when the chains are listed and no rule is present in a new created chain (repopeted in LP#1922892). <p>This code is backwards compatible, that means it works with the legacy "ebtables" binary; this is currently installed in the Neutron CI [1]. In order to test with the new binary, "ebtables-nft", two new CI jobs are added to the periodic queue [2].</p> <p>[1]https://github.com/openstack/neutron/blob/1ad9ca56b07ffdc9f7e0bc6a62af61961b9128eb/roles/legacy_ebtables/tasks/main.yaml [2]https://review.opendev.org/c/openstack/neutron/+785144</p> <p>Closes-Bug: #1922892 Related-Bug: #1508155 Closes-Bug: #1938670</p> <p>Conflicts: neutron/tests/unit/plugins/ml2/drivers/linuxbridge/agent/test_arp_protect.py</p> <p>Change-Id: I9463b000f6f3e65aaf91d60b30f6c92c01e3baf (cherry picked from commit 0a931391d8990f3e654b4bfda24ae4119c609bbf)</p> <p>tags:added: in-stable-victoria tags:added: in-stable-ussuri</p>	

OpenStack Infra (hudson-openstack) wrote on 2021-08-16: Fix merged to neutron (stable/ussuri)	#13
<p>Reviewed: https://review.opendev.org/c/openstack/neutron/+804057 Committed: https://opendev.org/openstack/neutron/commit/f034de001ba224c3add364ca5d00cc15e26c2e96 3add364ca5d00cc15e26c2e96 Submitter: "Zuul (22348)" Branch: stable/ussuri</p> <p>commit f034de001ba224c3add364ca5d00cc15e26c2e96 Author: Rodolfo Alonso Hernandez <email address hidden> Date: Wed Apr 7 13:16:21 2021 +0000</p> <p>Make ARP protection commands compatible with "ebtables-nft"</p> <p>"nftables" compatible binary, "ebtables-nft", is not 100% compatible with the legacy API, as reported in LP#1922892.</p> <p>This patch fixes the following issues when using "ebtables-nft" (while keeping compatibility with legacy binary):</p> <ul style="list-style-type: none">- When a new chain is created, a default DROP rule is added at the end of the chain (append). This will prevent the error code 4 when the chain is listed.- The chain rules are added at the begining of the chain (insert), before the default DROP rule. This will prioritize the port rules.- The MAC rules are cleaned before the new ones are added. That will prevent the deletion of any new needed rule, now added after the deletion.- The "ebtables" command will retry on error code 4. This is the error returned when the chains are listed and no rule is present in a new created chain (repopeted in LP#1922892). <p>This code is backwards compatible, that means it works with the legacy "ebtables" binary; this is currently installed in the Neutron CI [1]. In order to test with the new binary, "ebtables-nft", two new CI jobs are added to the periodic queue [2].</p> <p>[1]https://github.com/openstack/neutron/blob/1ad9ca56b07ffdc9f7e0bc6a62af61961b9128eb/roles/legacy_ebtables/tasks/main.yaml [2]https://review.opendev.org/c/openstack/neutron/+785144</p>	

Nahian Chowdhury
Nate
Nate Johnston
Naved Ali
Naved Ali Shah
Nitish
Normen Scholtke
Oleg Bondarev
OpenStack Vulnera...
Ozgur Kara
Pallavi
Paul Halmos
Paul Voccio
Pavani_addanki
Perry Waldner
Piyanai Saowarat...
Piyush Pathak
Pradeep Naik
Pradeep Roy Kandr...
Pramod
Prateek
Praveen Kumar SM
Prithiv
Prosunjit Biswas
Rajesh Battala
Rajesh Mohan
Raju Alluri
Ralf Trezeciak
Ranjit Ray
RaoFei
Ravi Chunduru
Ravim Singh
Rayman Lwo
Reedlip
Richa
Rick Melick
Robert Love
Rochelle Grober
Rodolfo Alonso
Roman Goncharov
Ron Cannella
Rudra Rugge
Ryan Tidwell
Ryo Shi
Ryu Ishimoto
SANTOSH KUMAR PAN...
ST Wang
Saisrikiran Mudig...
Samuel Bercovici
Sandeep Bisht
Sapna Jadhav
Satyanarayana Pat...
Sean McCully
Sebastian Luna-Va...
Shawn Hartsock
Shraddha Pandhe
Shruthi Chari
Shweta P
Sid Sun
Simon
Sindhu Devale
Slawek Kaplonski
Somik Behera
Songhee Kang
Songlian Li
Soo Choi
Sridhar Gaddam
Steve Sloka
Steven Pavlon
Stuart Hart
Sumit Naiksatam
Summer Long
Suraj Deshmukh
Sushma Korati
Swaminathan Vasud...
Swaroop Jayanthi
Takashi Kajinami
Tamas Kapolnasi
Tao Zhou
Taurus Cheung
Tayaa Med Amine
Thongth
Tiago Everton Fer...
Tony Tan
Tushar Patil
Uma
Vidhisha Nair
Vikas Deolalikar
Vinod Kumar
Vinu Pillai

<div>Closes-Bug: #192892</div> <div>Related-Bug: #1508155</div> <div>Closes-Bug: #1938670</div> <div>Conflicts:<div>neutron/tests/unit/plugins/ml2/drivers/linuxbridge/agent/test_arp_protect.py</div></div> <div>Change-Id: I9463b000f6f63e65aaf91d60b30f6c92c01e3baf</div> <div>(cherry picked from commit 0a931391d8990f3e654b4bfd24ae4119c609bbf)</div> <div>(cherry picked from commit fafa5dacd5057120562184a734e7345e7c0e9639)</div> <div>tags:added: in-stable-train</div>
--

OpenStack Infra (hudson-openstack) wrote on 2021-08-16: Fix merged to neutron (stable/train)	#14
<div>Reviewed: https://review.opendev.org/c/openstack/neutron/+804058</div> <div>Committed: https://opendev.org/openstack/neutron/commit/4245963c71280bebd94e9005230d610931a7c2df</div> <div>Submitter: "Zuul (22348)"</div> <div>Branch: stable/train</div> <div>commit 4245963c71280bebd94e9005230d610931a7c2df</div> <div>Author: Rodolfo Alonso Hernandez <email address hidden></div> <div>Date: Wed Apr 7 13:16:21 2021 +0000</div> <div>Make ARP protection commands compatible with "ebtables-nft"</div> <div>"nftables" compatible binary, "ebtables-nft", is not 100% compatible with the legacy API, as reported in LP#1922892.</div> <div>This patch fixes the following issues when using "ebtables-nft" (while keeping compatibility with legacy binary):</div> <div>- When a new chain is created, a default DROP rule is added at the end of the chain (append). This will prevent the error code 4 when the chain is listed.</div> <div>- The chain rules are added at the beginning of the chain (insert), before the default DROP rule. This will prioritize the port rules.</div> <div>- The MAC rules are cleaned before the new ones are added. That will prevent the deletion of any new needed rule, now added after the deletion.</div> <div>- The "ebtables" command will retry on error code 4. This is the error returned when the chains are listed and no rule is present in a new created chain (reopreted in LP#1922892).</div> <div>This code is backwards compatible, that means it works with the legacy "ebtables" binary; this is currently installed in the Neutron CI [1]. In order to test with the new binary, "ebtables-nft", two new CI jobs are added to the periodic queue [2].</div> <div>[1]https://github.com/openstack/neutron/blob/1ad9ca56b07ffdc9f7e0bc6a62af61961b9128eb/roles/legacy_ebtables/tasks/main.yaml</div> <div>[2]https://review.opendev.org/c/openstack/neutron/+785144</div> <div>Closes-Bug: #1922892</div> <div>Related-Bug: #1508155</div> <div>Closes-Bug: #1938670</div> <div>Conflicts:<div>neutron/tests/unit/plugins/ml2/drivers/linuxbridge/agent/test_arp_protect.py</div></div> <div>Change-Id: I9463b000f6f63e65aaf91d60b30f6c92c01e3baf</div> <div>(cherry picked from commit 0a931391d8990f3e654b4bfd24ae4119c609bbf)</div> <div>(cherry picked from commit fafa5dacd5057120562184a734e7345e7c0e9639)</div>	

OpenStack Infra (hudson-openstack) wrote on 2021-08-17: Fix merged to ossa (master)	#15
<div>Reviewed: https://review.opendev.org/c/openstack/ossa/+804116</div> <div>Committed: https://opendev.org/openstack/ossa/commit/5bfba3e739b9988206a51fc564a05cc32b23a791</div> <div>Submitter: "Zuul (22348)"</div> <div>Branch: master</div> <div>commit 5bfba3e739b9988206a51fc564a05cc32b23a791</div> <div>Author: Jeremy Stanley <email address hidden></div> <div>Date: Tue Aug 10 16:41:27 2021 +0000</div> <div>Add OSSA-2021-004 (CVE-2021-38598)</div> <div>Change-Id: I91b44e7fab3209170efd8dc594cb1b442ee48c2d</div> <div>Closes-Bug: #1938670</div> <div>Changed in ossa:</div> <div>status:In Progress → Fix Released</div>	

Jeremy Stanley (fungi) on 2021-08-17
summary: - Linuxbridge ARP filter bypass on Netfilter platforms (CVE-2021-38598) <div>+ [OSSA-2021-004] Linuxbridge ARP filter bypass on Netfilter platforms</div> <div>+ (CVE-2021-38598)</div>

Jeremy Stanley (fungi) wrote on 2021-08-17:	#16
I've distributed the advisory for this to relevant mailing lists now.	

OpenStack Infra (hudson-openstack) wrote on 2021-09-10: Fix included in openstack/neutron 16.4.1	#17
This issue was fixed in the openstack/neutron 16.4.1 release.	

OpenStack Infra (hudson-openstack) wrote on 2021-09-10: Fix included in openstack/neutron 17.2.1	#18
This issue was fixed in the openstack/neutron 17.2.1 release.	

Slawek Kaplonski (slaweq) on 2022-04-05
Changed in neutron:

Vishal Agarwal

Vivekanandan maha...

Wajid Baig

Xiang Hui

Xiaolin Zhang

Xin Zhong

YAMAMOTO Takashi

Yahoo! Engineerin...

Yang Yu

Yapeng Wu

Yi Yang

Yi Yang

Yogesh Mulay

Yongqiang Yang

Yushiro FURUKAWA

Yusuf G ng r

Yuxin Zhuang

Zahid Hasan

ZhangNi

Zhengwei Gao

Ziv

Zou Keke

ammarun

aprilcxn

avinashsau

ayyalaraju chalam...

ballin.zhang

balajipatnala

brightson

bugtracker@devshe...

bychyahoo@gmail.com

chaiwat wannaposop

chitu

congge

denghui huang

devin.li

diroguan

dql

droom

eroc Jiang

Fei Yang

galeido

gsccc

herrold

hideki takashima

ipenstack

jaychj

jeff wang

jiangjunyong

jinpengcheng

jyilifeng

jordan tardif

kalim khuang

kgrvamsi

kiriti

kkup

lanpi

laoyi

liaonanhai

lilintan

lin_victor

liuyang

lololmarwa255

lpmqtt

lpzh

maestropandy

manish

mayu

mayu

mershard frierson

miralaunchpad

mohit.048

monika

nawawit kes

pawan

pawnesh kumar

qinhaizhong

raja

ratalevolamena

satyanarayana pat...

satyanarayana pat...

sharko.cheng

sivagnanam C

sowmini

sunil

sunilcn

sunxifa

tangfeixiong

venkata anil

vivek.ys

status:Confirmed → Fix Released

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

[See full activity log](#)

[vividh siddha](#)
[wanghuagong](#)
[wushaohan](#)
[xianliangchi](#)
[xiaoningli](#)
[xreuze](#)
[yalei wang](#)
[yangbo](#)
[yangjianfeng](#)
[yangkai](#)
[yangzhenyu](#)
[yilong](#)
[yinpeijun](#)
[yongxiangwang](#)
[zhaobo](#)
[zhu zhu](#)
[zzfancy](#)

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

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