# [OSSA-2021-005] Arbitrary dnsmasq reconfiguration via extra_dhcp_opts (CVE-2021-40085)

Bug #1939733 reported by Pavel Toporkov on 2021-08-12

This bug affects 1 person 276

| Affects | Status | Importance | Assigned to | Milestone |
|---|---|---|---|---|
| OpenStack Security Advisory | Fix Released | High | Jeremy Stanley | |
| Ubuntu Cloud Archive | New | Undecided | Unassigned | |
| Queens | Fix Released | Undecided | Unassigned | |
| Rocky | Fix Released | Undecided | Unassigned | |
| Stein | Fix Released | Undecided | Unassigned | |
| Train | Fix Committed | Undecided | Unassigned | |
| Ussuri | Fix Committed | Undecided | Unassigned | |
| Victoria | Fix Committed | Undecided | Unassigned | |
| Wallaby | Fix Committed | Undecided | Unassigned | |
| Xena | New | Undecided | Unassigned | |
| neutron | Fix Released | Critical | Slawek Kaplonski | |
| neutron (Ubuntu) | Fix Released | Undecided | Unassigned | |
| Bionic | New | Undecided | Unassigned | |
| Focal | Fix Released | Undecided | Unassigned | |
| Hirsute | Won't Fix | Undecided | Unassigned | |
| Impish | Fix Released | Undecided | Unassigned | |

## Bug Description

Application doesnt check the input values for extra_dhcp_opts port parameter allowing user to use a newline character. The values from extra_dhcp_opts are used in rendering of opts file which is passed to dnsmasq as a dhcp-optsfile. Considering this, an attacker can inject any options to that file.

The main direct impact in my opinion is that attacker can push arbitrary dhcp options to another instances connected to the same network. And due to we are able to modify our own port connected to external network, it is possible to push dhcp options to the instances of another tennants using the same external network.

If we go further, there is an known buffer overflow vulnerability in dnsmasq (https://thekelleys.org.uk/gitweb/?p=dnsmasq.git;a=commitdiff;h=7d04e17444793a840f98a0283968b96502b112dc) which was not considered as a security issue due to attacker cannot control dhcp opts in most cases and therefore this vulnerability is still exists in most distributives (e.g Ubuntu 20.04.1). In our case dhcp opts is exactly what attacker can modify, so we can trigger buffer overflow there. I even managed to write an exploit which lead to a remote code execution using this buffer overflow vulnerability.

Here the payload to crash dnsmasq as a proof of concept:

```
PUT /v2.0/ports/9db67e0f-537c-494a-a655-c8a0c518d57e HTTP/1.1
Host: openstack
X-Auth-Token: TOKEN
Content-Type: application/json
Content-Length: 170

{"port":{
"extra_dhcp_opts":[{"opt_name":"zzz",
"opt_value":"xxx\n128,aa:bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
bbbbbbbbbbbbbbbbbbbbbbbbbbbb\n120,aa.cc\n128,:"
}]}}
```

Tested on ocata, train and victoria versions.

Vulnerability was found by Pavel Toporkov

See original description

Tags: patch

## CVE References

2021-40085

Jeremy Stanley (fungi) wrote on 2021-08-12: #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.

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

Slawek Kaplonski (slaweq) wrote on 2021-08-16: #2

Thx for reporting it. It seems like it should be private for now. I will work on it.

Changed in neutron:
**assignee**:nobody → Slawek Kaplonski (slaweq)

Slawek Kaplonski (slaweq) wrote on 2021-08-17: #3

Fix v1 (3.5 KiB, text/plain)

Fix like that can be backported to stable branches. In the future we may
propose fix on the API side (in neutron-lib) to remove such newline chars
before saving them in db.

Rodolfo Alonso (rodolfo-alonso-hernandez) wrote on 2021-08-17: #4

@Slawek, I would split the opt_value string each time, instead of removing
the "\n". That will take only the first part of the string, removing the
tail.

>>> opt_value = "xxx\n128,aa:bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb
bbbbbbbbbbbbbbbbbbbbbbbbbbbbb\n120,aa.cc\n128,:"
>>> opt_value.split()[0]
"xxx"

Slawek Kaplonski (slaweq) wrote on 2021-08-17: #5

Fix v2 (3.6 KiB, text/plain)

@Rodolfo, thx for review of the patch. I prepared new version of the
patch. Please check it.

Jeremy Stanley (fungi) wrote on 2021-08-17: #6

Naive question, but can the same bug be exploited with other characters
besides linefeed? Maybe carriage returns (\r), form feeds (\f), or
vertical tabs (\v) are treated similarly by dnsmasq?

Pavel Toporkov (paul-axe) wrote on 2021-08-18: **Re: [Bug 1939733] Re: Remote Code Execution via extra_dhcp_opts** #7

Download full text (3.6 KiB)
dnsmasq reads the config file using `fgets` functions, so it depends on
its
implementation. As far as i know, the default glibc supports only \n
character as a line delimiter

On Tue, Aug 17, 2021 at 6:41 PM Jeremy Stanley <email address hidden>
wrote:

[ . . . ]

Read more...

Jeremy Stanley (fungi) wrote on 2021-08-18: **Re: Remote Code Execution via extra_dhcp_opts** #8

Thanks. I suppose my remaining concern is more of a theoretical one in
that case... dnsmasq does not expect untrusted users to supply
configuration, and therefore is not overly concerned with risks related to
that workflow. As a result, any bugs in dnsmasq's configuration handling
become Neutron security risks and therefore OpenStack's responsibility to
deal with. In the long term, this does not seem like a sustainable model
under which to operate.

In the near term, I agree the proposed solution should suffice, and since
it seems to be backportable to all supported stable branches I'll get
started on the impact description and coordinated disclosure timeline for
an embargoed security advisory.

Changed in ossa:
    **status**:Incomplete → Confirmed
**importance**:Undecided → High
  **assignee**:nobody → Jeremy Stanley (fungi)

Jeremy Stanley (fungi) wrote on 2021-08-19: #9

Here's an initial draft for an impact description. Please review and
comment. If this summary reasonably captures the vulnerability, I'll use
it as the basis for our CVE request to MITRE, notification to downstream
stakeholders, and eventual security advisory. Also, Pavel, please let me
know if you have any organization you want credited with the discovery
alongside your name.

Title: Exposure of dnsmasq buffer overflow via extra_dhcp_opts
Reporter: Pavel Toporkov
Products: Neutron
Affects: <16.4.1, >=17.0.0 <17.2.1, >=18.0.0 <18.1.1

Description:
Pavel Toporkov reported a vulnerability in Neutron. By supplying a
specially crafted extra_dhcp_opts value, an authenticated user may trigger
a configuration parsing buffer overflow in some older versions of dnsmasq,
resulting in denial of service or remote code execution on the hosts where
dnsmasq is running. Only deployments with dnsmasq prior to 2.81 or without
commit 7d04e17 applied are affected.

Jeremy Stanley (fungi) wrote on 2021-08-19: #10

On revisiting the initial bug description, I see that I've failed to
capture the aspect where the user can also append lines for other
configuration outside the options list itself. I'll try to come up with a
better summary incorporating that.

Jeremy Stanley (fungi) wrote on 2021-08-19: #11

Here's a revised impact description:

Dan Sneddon
Daniel Alvarez
Dave Cahill
David
David Lapsley
David M. Zendzian
David Seelbach
Davish Bhardwaj
Debian PTS
Deepak Nair
DengBO
Dincer Celik
Dmitriev Artem An...
Dmitriy Andrushko
Dong Jun
Dongwon Cho
Doraann2
Douglas Mendizábal
Duc Nguyen
Dustin Lundquist
Edgar Magana
Edward
Elena Ezhova
Elvira García Ruiz
Euler Jiang
Evgeny Fedoruk
Flavio Fernandes
Florin Vinti
Fontenay Tony
Franko Fang
Gage Hugo
Gandharva
Ganesh Kadam
Ganesh Navgire
Gary Kotton
Gheza
Greg Althaus
Guangya Liu (Jay ...
HENG ZHANG
HaifengLi
Hampapur Ajay
Hao Wang
Harikrishna S
Harkirat Singh
Harsh Prasad
HaySayCheese
Hemant Jadhav
Hemanth Ravi
Hidagawa
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 Dennis
James Denton
Jared R Greene
Jay Janardhan
Jeff Ward
Jeremy Stanley
Jesse Jones
Jiajun Liu
Jie Li
Jinlai Shan
Joel wineland
John
John Buswell
John Davidge
John Kasperski
John Lenihan
John Perkins
Jordan Rinke
Joshua Padman
José Alfonso
Kausal Malladi
Kausum Kumar
Ken'ichi Ohmichi
Kenji Motohashi
Kent Liu
Kevin Benton
Kunal.Yadav
LIU Yulong
Lajos Katona
Le Tian Ren
Lei Zhang

Title: Exposure of dnsmasq buffer overflow via extra_dhcp_opts
Reporter: Pavel Toporkov
Products: Neutron
Affects: <16.4.1, >=17.0.0 <17.2.1, >=18.0.0 <18.1.1

Description:
Pavel Toporkov reported a vulnerability in Neutron. By supplying a specially crafted extra_dhcp_opts value, an authenticated user may add arbitrary configuration to the dnsmasq process in order to crash the service, change parameters for other tenants sharing the same interface, or otherwise alter that daemon's behavior. This vulnerability may also be used to trigger a configuration parsing buffer overflow in versions of dnsmasq prior 2.81, which could lead to remote code execution. All Neutron deployments are affected.

Jeremy Stanley (fungi) wrote on 2021-08-19: #12

I also meant to redo the title. How's this?

Title: Arbitrary dnsmasq reconfiguration via extra_dhcp_opts

Jeremy Stanley (fungi) wrote on 2021-08-19: #13

I also seem to have introduced a typo in the penultimate sentence, that should say "versions of dnsmasq prior to 2.81" (I somehow lost the "to" in the most recent revision).

Pavel Toporkov (paul-axe) wrote on 2021-08-20: #14

I reviewed the description and it seems to be OK.

Jeremy Stanley (fungi) wrote on 2021-08-20: #15

Thanks Pavel, also please let me know if you have any organization you want credited with the discovery alongside your name.

Slawek: Rodolfo: If the patch in comment #5 is deemed a sufficient fix for master (Xena), then once someone attaches viable backports for stable/wallaby, stable/victoria, and stable/ussuri branches, I'll schedule a disclosure date and prepare notification under embargo for our downstream stakeholders (distribution package maintainers, public cloud security contacts, and so on).

Pavel Toporkov (paul-axe) wrote on 2021-08-20: #16

No, please credit only my name there

Jeremy Stanley (fungi) wrote on 2021-08-22: #17

Okay, this is what I'll use to request a CVE assignment from MITRE. Once viable backports for stable/wallaby, stable/victoria, and stable/ussuri branches are attached, I'll schedule a disclosure date and prepare notification under embargo for our downstream stakeholders...

Title: Arbitrary dnsmasq reconfiguration via extra_dhcp_opts
Reporter: Pavel Toporkov
Products: Neutron
Affects: <16.4.1, >=17.0.0 <17.2.1, >=18.0.0 <18.1.1

Description:
Pavel Toporkov reported a vulnerability in Neutron. By supplying a specially crafted extra_dhcp_opts value, an authenticated user may add arbitrary configuration to the dnsmasq process in order to crash the service, change parameters for other tenants sharing the same interface, or otherwise alter that daemon's behavior. This vulnerability may also be used to trigger a configuration parsing buffer overflow in versions of dnsmasq prior to 2.81, which could lead to remote code execution. All Neutron deployments are affected.

Akihiro Motoki (amotoki) wrote on 2021-08-23: #18

The proposed fix no longer allows the reported security issue, but can we block it at the API level too?
If the neutron API does not allow multi-line string in the API level, we can block it for further API operations.

Note that we need to consider such extra_dhcp_options is already injected, so the proposed fix is required and it looks good.

Perhaps blocking it at the API level is optional so it can be done as a follow-up after the proposed fix is applied.
What in my mind is to implement a validator like below in the API level.

```
def _validate_oneline_string(data, max_len=None):
    msg = validators.validate_string(data, max_len)
    if msg:
        return msg
    lines = data.splitlines()
    if lines and lines[0] != data:
        msg = _("Multi-line string is not allowed: '%s'") % data
        LOG.debug(msg)
        return msg
```

Slawek Kaplonski (slaweq) wrote on 2021-08-23: #19

Fix v2 for stable/wallaby (3.6 KiB, text/plain)

Stable/wallaby backport

Slawek Kaplonski (slaweq) wrote on 2021-08-23: #20

Fix v2 for stable/victoria (3.6 KiB, text/plain)

Stable/victoria backport

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 Sdvoijspa
Matt Joyce
Matt Wear
Matt j
Matthew Thode
Matvej Jurbin
Michael Rowland H...
Michael Tietz
Micheal Thompson
Miguel Lavalle
Mika Kohonen
Mohammed Kasim
Mohankumar
Mohit Malik
Mr. MInhaj
Murali Raju
Na Zhu
Nahian Chowdhury
Name Changed
Nate
Nate Johnston
Naved Ali
Naved Ali Shah
Nitish
Nobuto Murata
Normen Scholtke
Oleg Bondarev
OpenStack Vulnera...
Ozgur Kara
PCTeacher012
Pallavi
Paolo Topa
Paul Halmos
Paul Voccio
Pavani_addanki
Perry Waldner
Peter Bullert
Piyanai Saowaratt...
Piyush Pathak
Pradeep Naik
Pradeep Roy Kandru
Pramod
Prateek
Praveen Kumar SM
Prithiv
Prosunjit Biswas
Punnsa
Rajesh Battala
Rajesh Mohan
Raju Alluri
Ralf Trezeciak
Ranjit Ray
RaoFei
Ravi Chunduru
RaviM Singh
Rayman Lwo
Reedip
Richa
Richard Seguin
Richard Williams
Rick Melick
Rob Linc
Robert Love
Robin Wang
Rochelle Grober
Roman Goncharov
Ron Cannella
Rudra Rugge
Rudra Saraswat
Ryan Garrett
Ryan Harper
Ryan Tidwell

Slawek Kaplonski (slaweq) wrote on 2021-08-23: #21

Fix v2 for stable/ussuri (3.6 KiB, text/plain)

```
Stable/ussuri backport
```

Slawek Kaplonski (slaweq) wrote on 2021-08-23: #22

```
@Akihiro - that was my idea also but I wanted to do it as next step later.
First I wanted to propose solution which can be easily backported.
When that will be solved, I can propose API level validation, some db
migration script for existing entries, etc. as a follow-up. Is that ok for
You?
```

Akihiro Motoki (amotoki) wrote on 2021-08-23: #23

```
@Slawek, it totally works for me. Thanks.
```

Jeremy Stanley (fungi) wrote on 2021-08-23: #24

```
Assuming I get a response from MITRE in the next 24 hours, I'd like to
schedule the coordinated disclosure (when we'll switch this bug to public
security and push the attached patches to Gerrit) for 15:00 UTC Tuesday
2021-08-31, a week from tomorrow. Is that date and time acceptable to
everyone?
```

Slawek Kaplonski (slaweq) wrote on 2021-08-24: #25

```
@Akihiro - thx.
@Jeremy - that works for me, thx a lot.
```

Akihiro Motoki (amotoki) on 2021-08-25

```
Changed in neutron:
importance:Undecided → Critical
```

Jeremy Stanley (fungi) on 2021-08-25

```
summary:- Remote Code Execution via extra_dhcp_opts
        + Arbitrary dnsmasq reconfiguration via extra_dhcp_opts (CVE-2021-40085)
```

Jeremy Stanley (fungi) wrote on 2021-08-25: **Re: Arbitrary dnsmasq reconfiguration via extra_dhcp_opts (CVE-2021-40085)** #26

```
Now that MITRE has responded with a CVE assignment, the proposed patches
(from comments #5, #19, #20, and #21) have been privately supplied to
downstream stakeholders along with a copy of the impact description (from
comment #17). We are still within our downstream notification window to be
able to proceed with coordinated disclosure at 15:00 UTC on 2021-08-31.
```

Jeremy Stanley (fungi) wrote on 2021-08-31: #27

```
Double-checking, is Slawek or one of the other Neutron core reviewers
available to get the fix and backports from comments #5, #19, #20, and #21
pushed to Gerrit in roughly half an hour (around 14:00 UTC)? That will
give me time to identify the change numbers for inclusion in the public
advisory scheduled to go out at 15:00 UTC.

If there's no one available, I'll push the patches to Gerrit myself, but
it would be better to have a Neutron core reviewer taking care of it and
also working on expedited approvals so we can get them merged as quickly
as possible (I can prioritize them in the gate pipeline once they're
approved, to speed things along even more).
```

Jeremy Stanley (fungi) wrote on 2021-08-31: #28

```
I heard back from Slawek in IRC and he's pushing the changes to Gerrit
now.

information type:Private Security → Public Security
     description:updated
         summary:- Arbitrary dnsmasq reconfiguration via extra_dhcp_opts (CVE-2021-40085)
                 + [OSSA-2021-005] Arbitrary dnsmasq reconfiguration via extra_dhcp_opts
                 + (CVE-2021-40085)
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-31: **Fix proposed to neutron (master)** #29

```
Fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/neutron/+/806746

Changed in neutron:
status:New → In Progress
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-31: **Fix proposed to neutron (stable/wallaby)** #30

```
Fix proposed to branch: stable/wallaby
Review: https://review.opendev.org/c/openstack/neutron/+/806748
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-31: **Fix proposed to neutron (stable/victoria)** #31

```
Fix proposed to branch: stable/victoria
Review: https://review.opendev.org/c/openstack/neutron/+/806749
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-31: **Fix proposed to neutron (stable/ussuri)** #32

Ryo Shi
Ryu Ishimoto
SANTOSH KUMAR PAN...
ST Wang
Sahid Orentino
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...
Swapnil Kulkarni
Swaroop Jayanthi
Takashi Kajinami
Tamas Kapolnasi
Tao Zhou
Taurus Cheung
Tayaa Med Amine
Thomas Martin
Thongth
Tiago Everton Fer...
Tom Weiss
Tony Tan
Tushar Patil
Ubuntu Cloud Arch...
Ubuntu OpenStack
Ubuntu Security Team
Uma
Vasanth
Vic Parker
Vidhisha Nair
Vikas Deolaliker
Vinod Kumar
Vinu Pillai
Vishal Agarwal
Vivekanandan maha...
Wajid Baig
Warren White
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 Güngör
Yuxin Zhuang
Zahid Hasan
ZhangNi
Zhengwei Gao
Ziv
Zou Keke
ahepas
ali
ammarun
aprilcxn
avinashsau
ayyalaraju chalam...
bailin.zhang
balajipatnala
basilisgabri
brightson
bugtracker@devshe...

Fix proposed to branch: stable/ussuri
Review: https://review.opendev.org/c/openstack/neutron/+/806750

OpenStack Infra (hudson-openstack) wrote on 2021-08-31: **Fix proposed to ossa (master)** #33

Fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/ossa/+/806754

Changed in ossa:
**status**:Confirmed → In Progress

OpenStack Infra (hudson-openstack) wrote on 2021-08-31: **Fix merged to ossa (master)** #34

Reviewed: https://review.opendev.org/c/openstack/ossa/+/806754
Committed: https://opendev.org/openstack/ossa/commit/55e0ee495344626
7d7900bda9cdfdc9f44a6b72d
Submitter: "Zuul (22348)"
Branch: master

commit 55e0ee4953446267d7900bda9cdfdc9f44a6b72d
Author: Jeremy Stanley <email address hidden>
Date: Tue Aug 31 13:56:02 2021 +0000

    Add OSSA-2021-005 (CVE-2021-40085)

    Change-Id: I58b8c608547e24ee144cab805d17c55045e4279a
    Closes-Bug: #1939733

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

Jeremy Stanley (fungi) wrote on 2021-08-31: #35

https://security.openstack.org/ossa/OSSA-2021-005.html is published,
announcements have been sent to the usual mailing lists, and MITRE has
been notified to switch the assigned CVE public.

OpenStack Infra (hudson-openstack) wrote on 2021-09-01: **Fix proposed to neutron (stable/train)** #36

Fix proposed to branch: stable/train
Review: https://review.opendev.org/c/openstack/neutron/+/806707

OpenStack Infra (hudson-openstack) wrote on 2021-09-01: **Fix proposed to neutron (stable/stein)** #37

Fix proposed to branch: stable/stein
Review: https://review.opendev.org/c/openstack/neutron/+/806708

OpenStack Infra (hudson-openstack) wrote on 2021-09-01: **Fix proposed to neutron (stable/rocky)** #38

Fix proposed to branch: stable/rocky
Review: https://review.opendev.org/c/openstack/neutron/+/806862

OpenStack Infra (hudson-openstack) wrote on 2021-09-01: **Fix proposed to neutron (stable/queens)** #39

Fix proposed to branch: stable/queens
Review: https://review.opendev.org/c/openstack/neutron/+/806709

Ubuntu Foundations Team Bug Bot (crichton) wrote on 2021-09-01: #40

The attachment "Fix v1" seems to be a patch. If it isn't, please remove
the "patch" flag from the attachment, remove the "patch" tag, and if you
are a member of the ~ubuntu-reviewers, unsubscribe the team.

[This is an automated message performed by a Launchpad user owned by
~brian-murray, for any issues please contact him.]

**tags**:added: patch

OpenStack Infra (hudson-openstack) wrote on 2021-09-02: **Fix merged to neutron (master)** #41

Reviewed: https://review.opendev.org/c/openstack/neutron/+/806746
Committed: https://opendev.org/openstack/neutron/commit/df891f0593d234e
01f27d7c0376d9702e178ecfb
Submitter: "Zuul (22348)"
Branch: master

commit df891f0593d234e01f27d7c0376d9702e178ecfb
Author: Slawek Kaplonski <email address hidden>
Date: Tue Aug 31 15:43:11 2021 +0200

    Remove dhcp_extra_opt value after first newline character

    Passing newline to the dnsmasq may cause security issues, especially
    that in case of Neutron that dhcp options' values are controlled by
    cloud users.
    This patch removes everything what is after first newline character
    in the dhcp_extra_opt's values before passing them to dnsmasq.

    Closes-Bug: #1939733
    Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e

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

OpenStack Infra (hudson-openstack) wrote on 2021-09-02: **Fix merged to neutron (stable/wallaby)** #42

Reviewed: https://review.opendev.org/c/openstack/neutron/+/806748
Committed: https://opendev.org/openstack/neutron/commit/35a32a1cadf2a6b
c182b3c7d7ae46e7cea73576a
Submitter: "Zuul (22348)"
Branch: stable/wallaby

bychyahoo@gmail.com
chaiwat wannaposop
chitu
congge
denghui huang
devin.li
diroguan
dql
droom
dsfkj dfjx
eoininmoran
eroc Jiang
fei Yang
galeido
ganesh
gsccc
herrold
hideki takashima
iopenstack
jaychj
jeff wang
jiangjunyong
jinpengcheng
jiyifeng
jordan tardif
kalim khuang
kgrvamsi
kiriti
kkup
lanpi
laoyi
liaonanhai
lilintan
lin_victor
linuxgijs
liuyang
lololmarwa255
lpmqtt
lzh
maestropandy
manish
mayu
mayu
mershard frierson
miralaunchpad
mmmen
mohit.048
monika
nawawit kes
nikonikic42
pawan
pawnesh kumar
projevie@hotmail.com
qadir
qinhaizhong
raja
ratalevolamena
sankaran
satyanarayana pat...
satyanarayana pat...
sharko.cheng
sivagnanam C
sowmini
sunil
sunilcn
sunxifa
tangfeixiong
ubuntu18
van
venkata anil
vivek.ys
vividh siddha
wanghuagong
wushaohan
xianliangchi
xiaoningli
xreuze
yalei wang
yangbo
yangjianfeng
yangkai
yangzhenyu
yilong
yinpeijun
yongxiangwang
zhaobo
zhu zhu
zzfancy

Patches

Fix v1
Fix v2
Fix v2 for stable/wallaby
Fix v2 for stable/victoria
Fix v2 for stable/ussuri
Add patch

```
commit 35a32a1cadf2a6bc182b3c7d7ae46e7cea73576a
Author: Slawek Kaplonski <email address hidden>
Date: Mon Aug 23 13:01:37 2021 +0200

    Remove dhcp_extra_opt value after first newline character

    Passing newline to the dnsmasq may cause security issues, especially
    that in case of Neutron that dhcp options' values are controlled by
    cloud users.
    This patch removes everything what is after first newline character
    in the dhcp_extra_opt's values before passing them to dnsmasq.

    Closes-Bug: #1939733
    Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e
    (cherry picked from commit df891f0593d234e01f27d7c0376d9702e178ecfb)
```

OpenStack Infra (hudson-openstack) wrote on 2021-09-02: **Fix merged to neutron (stable/victoria)** #43

```
Reviewed: https://review.opendev.org/c/openstack/neutron/+/806749
Committed: https://opendev.org/openstack/neutron/commit/a08e21c15b766a1
e3b2b64ae15f95565d9ea6688
Submitter: "Zuul (22348)"
Branch: stable/victoria

commit a08e21c15b766a1e3b2b64ae15f95565d9ea6688
Author: Slawek Kaplonski <email address hidden>
Date: Mon Aug 23 13:01:37 2021 +0200

    Remove dhcp_extra_opt value after first newline character

    Passing newline to the dnsmasq may cause security issues, especially
    that in case of Neutron that dhcp options' values are controlled by
    cloud users.
    This patch removes everything what is after first newline character
    in the dhcp_extra_opt's values before passing them to dnsmasq.

    Closes-Bug: #1939733
    Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e
    (cherry picked from commit df891f0593d234e01f27d7c0376d9702e178ecfb)
```

OpenStack Infra (hudson-openstack) wrote on 2021-09-07: **Fix merged to neutron (stable/ussuri)** #44

```
Reviewed: https://review.opendev.org/c/openstack/neutron/+/806750
Committed: https://opendev.org/openstack/neutron/commit/6ac5bc583787b7a
f6273d5344fcbeef69a48e2e3
Submitter: "Zuul (22348)"
Branch: stable/ussuri

commit 6ac5bc583787b7af6273d5344fcbeef69a48e2e3
Author: Slawek Kaplonski <email address hidden>
Date: Mon Aug 23 13:01:37 2021 +0200

    Remove dhcp_extra_opt value after first newline character

    Passing newline to the dnsmasq may cause security issues, especially
    that in case of Neutron that dhcp options' values are controlled by
    cloud users.
    This patch removes everything what is after first newline character
    in the dhcp_extra_opt's values before passing them to dnsmasq.

    Closes-Bug: #1939733
    Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e
    (cherry picked from commit df891f0593d234e01f27d7c0376d9702e178ecfb)
```

OpenStack Infra (hudson-openstack) wrote on 2021-09-09: **Fix merged to neutron (stable/rocky)** #45

```
Reviewed: https://review.opendev.org/c/openstack/neutron/+/806862
Committed: https://opendev.org/openstack/neutron/commit/e291dca5d97fc98
6fc7d85b8ea256a483d815277
Submitter: "Zuul (22348)"
Branch: stable/rocky

commit e291dca5d97fc986fc7d85b8ea256a483d815277
Author: Slawek Kaplonski <email address hidden>
Date: Mon Aug 23 13:01:37 2021 +0200

    Remove dhcp_extra_opt value after first newline character

    Passing newline to the dnsmasq may cause security issues, especially
    that in case of Neutron that dhcp options' values are controlled by
    cloud users.
    This patch removes everything what is after first newline character
    in the dhcp_extra_opt's values before passing them to dnsmasq.

    Conflicts:
        neutron/tests/unit/agent/linux/test_dhcp.py

    Closes-Bug: #1939733
    Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e
    (cherry picked from commit df891f0593d234e01f27d7c0376d9702e178ecfb)
```

OpenStack Infra (hudson-openstack) wrote on 2021-09-09: **Fix merged to neutron (stable/queens)** #46

```
Reviewed: https://review.opendev.org/c/openstack/neutron/+/806709
Committed: https://opendev.org/openstack/neutron/commit/110fed07cb83deb
3abd85073cb351066713b6384
Submitter: "Zuul (22348)"
Branch: stable/queens

commit 110fed07cb83deb3abd85073cb351066713b6384
Author: Slawek Kaplonski <email address hidden>
Date: Mon Aug 23 13:01:37 2021 +0200

    Remove dhcp_extra_opt value after first newline character

    Passing newline to the dnsmasq may cause security issues, especially
    that in case of Neutron that dhcp options' values are controlled by
    cloud users.
    This patch removes everything what is after first newline character
    in the dhcp_extra_opt's values before passing them to dnsmasq.

    Conflicts:
        neutron/tests/unit/agent/linux/test_dhcp.py
```

Closes-Bug: #1939733
Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e
(cherry picked from commit df891f0593d234e01f27d7c0376d9702e178ecfb)

OpenStack Infra (hudson-openstack) wrote on 2021-09-09: **Fix merged to neutron (stable/stein)** #47

Reviewed: https://review.opendev.org/c/openstack/neutron/+/806708
Committed: https://opendev.org/openstack/neutron/commit/e2d6e2d5d2388cd7c135a50129466aaa7ca85cbf
Submitter: "Zuul (22348)"
Branch: stable/stein

commit e2d6e2d5d2388cd7c135a50129466aaa7ca85cbf
Author: Slawek Kaplonski <email address hidden>
Date: Mon Aug 23 13:01:37 2021 +0200

Remove dhcp_extra_opt value after first newline character

Passing newline to the dnsmasq may cause security issues, especially
that in case of Neutron that dhcp options' values are controlled by
cloud users.
This patch removes everything what is after first newline character
in the dhcp_extra_opt's values before passing them to dnsmasq.

Closes-Bug: #1939733
Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e
(cherry picked from commit df891f0593d234e01f27d7c0376d9702e178ecfb)

OpenStack Infra (hudson-openstack) wrote on 2021-09-09: **Fix merged to neutron (stable/train)** #48

Reviewed: https://review.opendev.org/c/openstack/neutron/+/806707
Committed: https://opendev.org/openstack/neutron/commit/757d8c6e322eeda299aa5e055e38b1ed48977f2d
Submitter: "Zuul (22348)"
Branch: stable/train

commit 757d8c6e322eeda299aa5e055e38b1ed48977f2d
Author: Slawek Kaplonski <email address hidden>
Date: Mon Aug 23 13:01:37 2021 +0200

Remove dhcp_extra_opt value after first newline character

Passing newline to the dnsmasq may cause security issues, especially
that in case of Neutron that dhcp options' values are controlled by
cloud users.
This patch removes everything what is after first newline character
in the dhcp_extra_opt's values before passing them to dnsmasq.

Closes-Bug: #1939733
Change-Id: Ifeaf258f0b5ea86f25620ac4116d618980a7272e
(cherry picked from commit df891f0593d234e01f27d7c0376d9702e178ecfb)

OpenStack Infra (hudson-openstack) wrote on 2021-09-10: **Fix included in openstack/neutron 16.4.1** #49

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** #50

This issue was fixed in the openstack/neutron 17.2.1 release.

OpenStack Infra (hudson-openstack) wrote on 2021-09-10: **Fix included in openstack/neutron 18.1.1** #51

This issue was fixed in the openstack/neutron 18.1.1 release.

OpenStack Infra (hudson-openstack) wrote on 2021-09-15: **Fix included in openstack/neutron 19.0.0.0rc1** #52

This issue was fixed in the openstack/neutron 19.0.0.0rc1 release
candidate.

OpenStack Infra (hudson-openstack) wrote on 2021-09-29: **Related fix proposed to neutron-lib (master)** #53

Related fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/neutron-lib/+/811708

Christian Rohmann (christian-rohmann) wrote on 2021-10-11: #54

@Slawek are you also pushing the new packages to Ubuntu Cloud Archive?

i.e. https://openstack-ci-reports.ubuntu.com/reports/cloud-archive/ussuri_versions.html does not show any 16.4.1 as of yet.

Jeremy Stanley (fungi) wrote on 2021-10-11: #55

Slawek is one of the upstream Neutron developers. One of the Ubuntu
package maintainers will need to take care of Ubuntu's package updates.
It's probably mildly confusing that this bug report is marked as affecting
the upstream project (where it's been fixed for months) but also the
Ubuntu packages which still need the report triaged.

Bernard Cafarelli (bcafarel) on 2021-11-17

**tags**:added: neutron-proactive-backport-potential

OpenStack Infra (hudson-openstack) wrote on 2021-11-25: **Related fix merged to neutron-lib (master)** #56

Reviewed: https://review.opendev.org/c/openstack/neutron-lib/+/811708
Committed: https://opendev.org/openstack/neutron-lib/commit/1f4c4031ee8a0dc91149dc6a83c7051db7628f23
Submitter: "Zuul (22348)"
Branch: master

commit 1f4c4031ee8a0dc91149dc6a83c7051db7628f23
Author: Slawek Kaplonski <email address hidden>
Date: Wed Sep 29 12:34:17 2021 +0200

Add oneline_string validators

Those new validators are used to validate extra_dhcp_opt's opt_name
and
opt_value fields to not allow multi-line strings to be set there.

Related-Bug: #1939733
Change-Id: I4dc3a09847205a660dc966d8eabccb4946f9bbc6

Slawek Kaplonski (slaweq) on 2021-12-17

**tags**:removed: neutron-proactive-backport-potential

OpenStack Infra (hudson-openstack) wrote on 2022-01-13: **Related fix proposed to neutron (master)** #57

Related fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/neutron/+/824641

OpenStack Infra (hudson-openstack) wrote on 2022-01-19: **Related fix merged to neutron (master)** #58

Reviewed: https://review.opendev.org/c/openstack/neutron/+/824641
Committed: https://opendev.org/openstack/neutron/commit/ef97019c92e96d0
bb17785daaf570b04c68be500
Submitter: "Zuul (22348)"
Branch: master

commit ef97019c92e96d0bb17785daaf570b04c68be500
Author: Slawek Kaplonski <email address hidden>
Date: Thu Jan 13 20:35:53 2022 +0100

Add upgrade check for extra DHCP options

Some time ago with patches [1] and [2] we trimmed extra_dhcp_opt name
and value to first newline character before using them in the dnsmasq
and later added API validator to not allow such names and/or values
with
newline character in it at all.
This patch adds upgrade check to warn users if they have old entries
with newline characters in the database already.

Related-Bug: #1939733

[1] https://review.opendev.org/c/openstack/neutron/+/806746
[2] https://review.opendev.org/c/openstack/neutron-lib/+/811708

Change-Id: I9a45d918b5a90f8fc50a9ec43b2a67cf582eb369

Brian Murray (brian-murray) wrote on 2022-01-26: #59

The Hirsute Hippo has reached End of Life, so this bug will not be fixed
for that release.

Changed in neutron (Ubuntu Hirsute):
**status**:New → Won't Fix

Corey Bryant (corey.bryant) wrote on 2022-01-27: #60

Ubuntu CVE tracker: https://ubuntu.com/security/cve-2021-40085

Changed in neutron (Ubuntu):
**status**:New → Fix Released
Changed in neutron (Ubuntu Impish):
**status**:New → Fix Released
Changed in neutron (Ubuntu Focal):
**status**:New → Fix Released

OpenStack Infra (hudson-openstack) wrote on 2022-11-18: **Fix included in openstack/neutron queens-eol** #61

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

OpenStack Infra (hudson-openstack) wrote on 2022-11-18: **Fix included in openstack/neutron rocky-eol** #62

This issue was fixed in the openstack/neutron rocky-eol release.

OpenStack Infra (hudson-openstack) wrote on 2022-11-18: **Fix included in openstack/neutron stein-eol** #63

This issue was fixed in the openstack/neutron stein-eol release.

See full activity log

To post a comment you must log in.