Log in / Register

OpenStack Compute (nova)

Overview Code Bugs Blueprints Translations Answers

[OSSA-2021-002] Open Redirect in noVNC proxy (CVE-2021-3654)

Bug #1927677 reported by Swe W Aung on 2021-05-07

This bug affects 2 people

280

Affects	Status	Importance	Assigned to	Milestone
OpenStack Compute (nova)	Fix Released	Undecided	Unassigned	
Stein	In Progress	Undecided	Unassigned	
Train	Fix Committed	Undecided	Unassigned	
Ussuri	Fix Released	Undecided	Unassigned	
Victoria	Fix Released	Undecided	Unassigned	
Wallaby	Fix Released	Undecided	Unassigned	
OpenStack Security Advisory	Fix Released	Undecided	Unassigned	

Bug Description

```
This bug report is related to Security.

Currently novnc is allowing open direction, which could potentially be
used for phishing attempts

To test.
https://<sites' vnc domain>//example.com/%2F..
include .. at the end

For example:
http://vncproxy.my.domain.com//example.com/%2F..

It will redirect to example.com. You can replace example.com with some
legitimate domain or spoofed domain.

The description of the risk is
By modifying untrusted URL input to a malicious site, an attacker may
successfully launch a phishing scam and steal user credentials.
Because the server name in the modified link is identical to the original
site, phishing attempts may have a more trustworthy appearance.
```

See original description

Tags: console in-stable-ussuri in-stable-victoria in-stable-wallaby novnc

CVE References

2021-3654

Swe W Aung (sirswa) wrote on 2021-05-07: #1

```
You can also test from the host that running novnc service,

nova:~# curl -v 'http://127.0.0.1:6080//google.com/%2F..'
* Trying 127.0.0.1...
* TCP_NODELAY set
* Connected to 127.0.0.1 (127.0.0.1) port 6080 (#0)
> GET //google.com/%2F.. HTTP/1.1
> Host: 127.0.0.1:6080
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 301 Moved Permanently
< Server: WebSockify Python/3.6.9
< Date: Fri, 07 May 2021 04:49:39 GMT
< Location: //google.com/%2F../
* no chunk, no close, no size. Assume close to signal end
<
```

Jeremy Stanley (fungi) wrote on 2021-05-07: #2

```
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

melanie witt (melwitt) wrote on 2021-05-11: #3

```
This bug report reminds me of an old bug [1] we dealt with in the past
where the canned vnc_auto.html and vnc.html pages allowed injection of
arbitrary HTML into them (fixed in noVNC 0.6.2) [2].

vnc_auto.html (vnc_lite.html as of v1.0.0) and vnc.html have a feature
where a host and port can be specified as query parameters in the URL,
example [3]:

  http://1.2.3.4:6080/vnc_auto.html?host=6.7.8.9&port=6080

and it will connect to a noVNC server running on that host:port as the
source of data provided to vnc_auto.html. The bug [2] meant that if a user
specified host:port in the URL query parameters, a potentially malicious
noVNC server running on that host:port could inject arbitrary HTML into
the vnc_auto.html being served on the user's machine.

I mention that because it seems like the host:port functionality could be
similarly used to phish. I'm thinking if someone ran their own noVNC
server at host:port and got a user to click on a link with ?host&port in
```

Report a bug

This report contains **Public Security** information

Everyone can see this security related information.

Duplicates of this bug

Bug #1988302

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
Joshua Padman
Matteo Pozza
Nova Core securit...
Sam Morrison
Shahaan Ayyub
Summer Long
Swe W Aung
melanie witt

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
Andy Southgate
Anna
Anthony Young
Antony Francis Ma...
April Wang
Arpita Rathi
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
Deepak Nair
DengBO
Derek Ragona
Devdeep Singh
Donghoon Kim

it, they could steal credentials if the user didn't notice what machine they're connecting to.

If that's the case, I'm not sure this redirect behavior is much different than what is already built-in to the vnc_lite.html and vnc.html pages that come with noVNC.

Aside from that, it's not clear to me whether this redirect behavior is something we (nova) control or if it's being done by noVNC itself. If it's the latter, I'm not sure whether we could do anything to intercept it or if it's something that would have to be changed in noVNC.

I'm going to add noVNC to this bug to get their input about the redirect behavior.

[1] https://bugs.launchpad.net/horizon/+bug/1656435
[2] https://github.com/novnc/noVNC/issues/748
[3] https://github.com/novnc/noVNC/blob/v1.1.0/vnc_lite.html#L14-L15

melanie witt (melwitt) wrote on 2021-05-11: #4

> I'm going to add noVNC to this bug to get their input about the redirect behavior.

Looks like I can't do that because noVNC and websockify use github issues and those can't be private security. But if it is indeed an issue in noVNC or websockify, then it is probably OK to go ahead and report it publicly in those projects.

I'm going to do some local testing to determine whether this redirect is something we could intercept and handle or if it happens before we (websockify plugin) are called. If it doesn't appear we can intercept it, we can switch this to public and I can report an issue for noVNC or websockify on github.

melanie witt (melwitt) wrote on 2021-05-12: #5

lp1927677.patch (1.6 KiB, text/plain)

OK, I really went down the rabbit hole with this one.

The tl;dr is that this is a known issue in the python standard library [1], in the http.server.SimpleHTTPRequestHandler, which WebSockifyRequestHandler derives from and which we ultimately derive from with our NovaProxyRequestHandler.

I found that we _can_ intercept this in our code and prevent an open redirect. It could be considered hacky, but I'm attaching a patch that prevents the redirect. It is code copied from a comment on the python issue [2].

The concern about the sample code in the issue is that such code might reject legitimate requests in certain cases. I don't believe we have such a concern with the nova console proxy.

Let me know what you think.

[1] https://bugs.python.org/issue32084
[2] https://bugs.python.org/issue32084#msg306545

melanie witt (melwitt) wrote on 2021-05-12: #6

Also, I'm thinking we could make this bug public considering the root cause of the behavior is a public issue in the python standard http.server.SimpleHTTPRequestHandler.

melanie witt (melwitt) wrote on 2021-05-12: #7

Also, I have tested the patch in comment 5 in devstack and verified it works to return a 400 Bad Request if "//" are included in the URL to redirect, provided that the browser has not previously cached a past redirect.

I used the following URL to test: http://127.0.0.1:6080//google.com/%2F..

Jeremy Stanley (fungi) on 2021-05-13

description:updated
information type:Private Security → Public
information type:Public → Public Security

Jeremy Stanley (fungi) wrote on 2021-05-13: #8

Thanks for digging into this, Melanie! I've ended the embargo and switched to Public Security given the relatively low risk this represents and its relationship with known issues in WebSockify/stdlib.

If the patch is sufficient and gets backported to stable branches, we could issue an advisory (class A in our report taxonomy). We could also consider it a workaround for a bug in a dependency (class C2), but that gets into determining whether the vulnerability is in the dependency or merely in the way we're using it. I'll leave the security advisory task incomplete for the time being, and we'll see how the fix progresses in review.

OpenStack Infra (hudson-openstack) wrote on 2021-05-13: **Fix proposed to nova (master)** #9

Fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/nova/+/791297

Changed in nova:
status:New → In Progress

melanie witt (melwitt) on 2021-05-13

tags:added: console

Dongwon Cho
Douglas Mendizábal
Dustin Lundquist
Ed Villalovoz
Eric Kwon
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
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
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
Piyanai Saowaratt...
Pradeep Roy Kandru
Pranali Deore
Prateek
Prithiv Mohan
Prosunjit Biswas
Rafi Khardalian
Rajesh Battala
Raju Alluri

Swe W Aung (sirswa) wrote on 2021-05-14: **Re: [Bug 1927677] Re: novnc allowing open direction which could potentially be used for phishing** #10

Hi Melanie

The is for the investigation and your effort. Really appreciate that.

Regards
sw3

On Sat, 15 May 2021 at 1:06 am, melanie witt <email address hidden>
wrote:

[...]

Swe W Aung (sirswa) wrote on 2021-05-14: #11

Hi Melanie

Thanks for the investigation and the effort. Really appreciate that.

Regards
sw3

On Sat, 15 May 2021 at 7:10 am, Swe Win Aung <email address hidden> wrote:

[...]

melanie witt (melwitt) wrote on 2021-05-15: **Re: novnc allowing open direction which could potentially be used for phishing** #12

Hi sw3,

Thanks for reporting the issue!

OpenStack Infra (hudson-openstack) wrote on 2021-05-15: **Fix merged to nova (master)** #13

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/791297
Committed: https://opendev.org/openstack/nova/commit/781612b33282ed2
98f742c85dab58a075c8b793e
Submitter: "Zuul (22348)"
Branch: master

commit 781612b33282ed298f742c85dab58a075c8b793e
Author: melanie witt <email address hidden>
Date: Thu May 13 05:43:42 2021 +0000

    Reject open redirection in the console proxy

    Our console proxies (novnc, serial, spice) run in a websockify server
    whose request handler inherits from the python standard
    SimpleHTTPRequestHandler. There is a known issue [1] in the
    SimpleHTTPRequestHandler which allows open redirects by way of URLs
    in the following format:

      http://vncproxy.my.domain.com//example.com/%2F..

    which if visited, will redirect a user to example.com.

    We can intercept a request and reject requests that pass a redirection
    URL beginning with "//" by implementing the
    SimpleHTTPRequestHandler.send_head() method containing the
    vulnerability to reject such requests with a 400 Bad Request.

    This code is copied from a patch suggested in one of the issue
comments
    [2].

    Closes-Bug: #1927677

    [1] https://bugs.python.org/issue32084
    [2] https://bugs.python.org/issue32084#msg306545

    Change-Id: Ie36401c782f023d1d5f2623732619105dc2cfa24
```

Changed in nova:
status:In Progress → Fix Released

OpenStack Infra (hudson-openstack) wrote on 2021-05-15: **Fix proposed to nova (stable/wallaby)** #14

```
Fix proposed to branch: stable/wallaby
Review: https://review.opendev.org/c/openstack/nova/+/791577
```

OpenStack Infra (hudson-openstack) wrote on 2021-05-17: **Fix proposed to nova (stable/victoria)** #15

```
Fix proposed to branch: stable/victoria
Review: https://review.opendev.org/c/openstack/nova/+/791805
```

OpenStack Infra (hudson-openstack) wrote on 2021-05-17: **Fix proposed to nova (stable/ussuri)** #16

```
Fix proposed to branch: stable/ussuri
Review: https://review.opendev.org/c/openstack/nova/+/791806
```

OpenStack Infra (hudson-openstack) wrote on 2021-05-17: **Fix proposed to nova (stable/train)** #17

```
Fix proposed to branch: stable/train
Review: https://review.opendev.org/c/openstack/nova/+/791807
```

OpenStack Infra (hudson-openstack) wrote on 2021-06-19: **Fix merged to nova (stable/wallaby)** #18

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/791577
Committed: https://opendev.org/openstack/nova/commit/470925614223c8d
d9b1233f54f5a96c02b2d4f70
Submitter: "Zuul (22348)"
Branch: stable/wallaby

commit 470925614223c8dd9b1233f54f5a96c02b2d4f70
Author: melanie witt <email address hidden>
Date: Thu May 13 05:43:42 2021 +0000

    Reject open redirection in the console proxy
```

Ranjit Ray
Ratnaker
RaviM Singh
Ray Trejo
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
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
Valery Tschopp
Venkata Siva Vija...
Vidhisha Nair
Vilobh Meshram
Vinu Pillai
Vish Ishaya
Vladik Romanovsky
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

```
    Our console proxies (novnc, serial, spice) run in a websockify server
    whose request handler inherits from the python standard
    SimpleHTTPRequestHandler. There is a known issue [1] in the
    SimpleHTTPRequestHandler which allows open redirects by way of URLs
    in the following format:

      http://vncproxy.my.domain.com//example.com/%2F..

    which if visited, will redirect a user to example.com.

    We can intercept a request and reject requests that pass a redirection
    URL beginning with "//" by implementing the
    SimpleHTTPRequestHandler.send_head() method containing the
    vulnerability to reject such requests with a 400 Bad Request.

    This code is copied from a patch suggested in one of the issue
comments
    [2].

    Closes-Bug: #1927677

    [1] https://bugs.python.org/issue32084
    [2] https://bugs.python.org/issue32084#msg306545

    Change-Id: Ie36401c782f023d1d5f2623732619105dc2cfa24
    (cherry picked from commit 781612b33282ed298f742c85dab58a075c8b793e)
```

Jeremy Stanley (fungi) wrote on 2021-07-09: **Re: novnc allowing open direction which could potentially be used for phishing** #19

Since we have fixes for this merged to all maintained stable branches (and them some), we need to decide whether we're issuing a security advisory about this or merely treating it as hardening. Does anyone have an opinion?

melanie witt (melwitt) wrote on 2021-07-09: #20

The fix backports have been proposed but are not yet merged on stable/victoria, stable/ussuri, and stable/train.

This issue is considered to be of "moderate" severity and is a result of a publicly reported behavior in the python standard library [1] and the http.server documentation has a warning on it that states, "Warning http.server is not recommended for production. It only implements basic security checks." [2].

Our dependency however, the websockify server [3], is based upon http.server and AFAIK websockify isn't characterized as only for dev or non-production use.

There is currently a pull request proposed to fix [1] and it is currently under review [4].

Based on this, I tend to think to treat it as hardening, but of course I defer to the expert opinion of the VMT.

[1] https://bugs.python.org/issue43223
[2] https://docs.python.org/3/library/http.server.html
[3] https://github.com/novnc/websockify
[4] https://github.com/python/cpython/pull/24848

Joshua Padman (jpadman) wrote on 2021-07-12: #21

The last OSSA that was released was also for an open redirect.
https://security.openstack.org/ossa/OSSA-2020-008.html

Its not a fancy vulnerability but it is one that can lead to far more significant issues. Ideally a CVE would be assigned to this, though maybe in the interest of consistency an OSSA may be required too?

Jeremy Stanley (fungi) wrote on 2021-07-12: #22

Melanie: Thanks for pointing out that the backports for branches prior to stable/wallaby haven't merged yet; I misread the notifications. We can't publish an advisory anyway until those are merged for the maintained branches at a minimum (fixes for branches under extended maintenance can merge after any advisory though).

Joshua: As Melanie points out, what we're providing is a workaround for a known security flaw in a dependency, so differs slightly from OSSA-2020-008 in that regard. You are right though that the end result is roughly the same for vulnerable deployments, and unlike most vulnerabilities involving dependencies this is one we actually have an active mitigation for which doesn't require any additional action on the part of the deployer other than upgrading our software in the deployment (no additional configuration or dependency upgrade steps needed).

I'm disappearing on a week-long vacation tomorrow, but if someone wants to compose an impact description for this and request a CVE from MITRE with it (or assign one as a CNA), I'm happy to help coordinate any advisory when I get home. Our template for impact descriptions can be found here: https://security.openstack.org/vmt-process.html#impact-description

OpenStack Infra (hudson-openstack) wrote on 2021-07-15: **Fix included in openstack/nova 23.0.2** #23

This issue was fixed in the openstack/nova 23.0.2 release.

Nick Tait (nickthetait) wrote on 2021-07-23: **Re: novnc allowing open direction which could potentially be used for phishing** #24

Red Hat will be assigning a CVE for this. Sirswa, would you like to be credited as the reporter? What name should we put down? Do you represent an organization?

Shahaan Ayyub (shahaan) wrote on 2021-07-24: **Re: [Bug 1927677] Re: novnc allowing open direction which could potentially be used for phishing** #25

Thanks Nick,
  We are part of the Monash University Nectar Cloud team. Please feel free to put us reporters.

lica
lin han
liuwei
liuzhuangzhuang
lololmarwa255
lpmqtt
maestropandy
manish
mershard frierson
mimul
miralaunchpad
mohit.048
nawawit kes
phalgun sirga
raja
robin
sangbaobao
satyanarayana pat...
satyanarayana pat...
shadyabhi
sivagnanam C
soumiyajit
sunilcn
tangfeixiong
victorye81
vishwa
vivek.ys
vks1
wanghuagong
wangqiang.sheng
woody89
xianliangchi
xiaoningli
xreuze
ya.wang
yangbo
yangkai
yangzhenyu
yanxubin
yilong
yongxiangwang
yysimida
zhengyue
zhu zhu
zhuangkai.zong

Patches

lp1927677.patch

python2.patch

python3.patch

Add patch

Remote bug watches

python-roundup #32084
[2:2]

python-roundup #43223
[1:None]

auto-github-novnc-novnc #748
[closed bug]

Bug watches keep track of this bug in other bug trackers.

Swe Aung
Shahaan Ayyub

Regards,
Shahaan

On Sat, 24 Jul 2021 at 09:25, Nick Tait <email address hidden> wrote:

[...]

Jeremy Stanley (fungi) wrote on 2021-07-24: **Re: novnc allowing open direction which could potentially be used for phishing** #26

Nick: Thanks for offering to assign a CVE for this. Do you have text for an impact description you'll be using in the CVE? If not, I can work on putting one together, though we still don't have any ETA on when the workarounds will merge to stable/victoria and earlier branches (and wouldn't issue a formal advisory until they do).

Swe W Aung (sirswa) wrote on 2021-07-26: #27

Hi Nick

Thanks. I noticed the CVE at RedHat few days ago. Thank you for following up and assigning at RedHat.

I will have to acknowledge Monash University Cyber Security team's vulnerability discovery work and raising the issue to us originally. I work for Monash University.

Our names are
Swe Aung
Shahaan Ayyub
Salman Khan (Cyber Security)

Thank you.

OpenStack Infra (hudson-openstack) wrote on 2021-07-26: **Fix merged to nova (stable/victoria)** #28

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/791805
Committed: https://opendev.org/openstack/nova/commit/6b70350bdcf59a9
712f88b6435ba2c6500133e5b
Submitter: "Zuul (22348)"
Branch: stable/victoria

commit 6b70350bdcf59a9712f88b6435ba2c6500133e5b
Author: melanie witt <email address hidden>
Date: Thu May 13 05:43:42 2021 +0000

    Reject open redirection in the console proxy

    Our console proxies (novnc, serial, spice) run in a websockify server
    whose request handler inherits from the python standard
    SimpleHTTPRequestHandler. There is a known issue [1] in the
    SimpleHTTPRequestHandler which allows open redirects by way of URLs
    in the following format:

      http://vncproxy.my.domain.com//example.com/%2F..

    which if visited, will redirect a user to example.com.

    We can intercept a request and reject requests that pass a redirection
    URL beginning with "//" by implementing the
    SimpleHTTPRequestHandler.send_head() method containing the
    vulnerability to reject such requests with a 400 Bad Request.

    This code is copied from a patch suggested in one of the issue
comments
    [2].

    Closes-Bug: #1927677

    [1] https://bugs.python.org/issue32084
    [2] https://bugs.python.org/issue32084#msg306545

    Conflicts:
        nova/console/websocketproxy.py
        nova/tests/unit/console/test_websocketproxy.py

    NOTE(melwitt): The conflicts are because the following changes are not
    in Victoria:

      Ib2c406327fef2fb4868d8050fc476a7d17706e23 (Remove six.moves)
      I58b0382c86d4ef798572edb63d311e0e3e6937bb (Refactor and rename
        test_tcp_rst_no_compute_rpcapi)

    Change-Id: Ie36401c782f023d1d5f2623732619105dc2cfa24
    (cherry picked from commit 781612b33282ed298f742c85dab58a075c8b793e)
    (cherry picked from commit 470925614223c8dd9b1233f54f5a96c02b2d4f70)
```

OpenStack Infra (hudson-openstack) wrote on 2021-07-27: **Fix merged to nova (stable/ussuri)** #29

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/791806
Committed: https://opendev.org/openstack/nova/commit/719e651e6be2779
50632e0c2cf5cc9a018344e7b
Submitter: "Zuul (22348)"
Branch: stable/ussuri

commit 719e651e6be277950632e0c2cf5cc9a018344e7b
Author: melanie witt <email address hidden>
Date: Thu May 13 05:43:42 2021 +0000

    Reject open redirection in the console proxy

    Our console proxies (novnc, serial, spice) run in a websockify server
    whose request handler inherits from the python standard
    SimpleHTTPRequestHandler. There is a known issue [1] in the
    SimpleHTTPRequestHandler which allows open redirects by way of URLs
    in the following format:

      http://vncproxy.my.domain.com//example.com/%2F..

    which if visited, will redirect a user to example.com.

    We can intercept a request and reject requests that pass a redirection
    URL beginning with "//" by implementing the
    SimpleHTTPRequestHandler.send_head() method containing the
    vulnerability to reject such requests with a 400 Bad Request.
    This code is copied from a patch suggested in one of the issue
comments
    [2].

    Closes-Bug: #1927677

    [1] https://bugs.python.org/issue32084
    [2] https://bugs.python.org/issue32084#msg306545

    Change-Id: Ie36401c782f023d1d5f2623732619105dc2cfa24
    (cherry picked from commit 781612b33282ed298f742c85dab58a075c8b793e)
    (cherry picked from commit 470925614223c8dd9b1233f54f5a96c02b2d4f70)
    (cherry picked from commit 6b70350bdcf59a9712f88b6435ba2c6500133e5b)
```

Jeremy Stanley (fungi) wrote on 2021-07-27: **Re: novnc allowing open direction which could potentially be used for phishing** #30

```
Actually, since the stable/train branch has transitioned from maintained
to extended maintenance status we no longer need to hold off any advisory
waiting for the fix there to merge. I'll go ahead and start drafting the
advisory now, since the stable/ussuri fix has merged.
```

```
Changed in ossa:
    status:Incomplete → In Progress
importance:Undecided → Medium
  assignee:nobody → Jeremy Stanley (fungi)
```

Jeremy Stanley (fungi) wrote on 2021-07-27: #31

```
Nick: What CVE number have you assigned for this? Or should I go ahead and
ask MITRE to assign one?
```

melanie witt (melwitt) wrote on 2021-07-27 (last edit on 2021-07-27): #32

```
I'm working on getting reviews for the backport patches, only the
stable/train patch remains.

(update) Oops, I just now see Jeremy's comment #30. Makes sense.
```

OpenStack Infra (hudson-openstack) wrote on 2021-07-27: **Fix proposed to ossa (master)** #33

```
Fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/ossa/+/802590
```

Jeremy Stanley (fungi) wrote on 2021-07-27: **Re: novnc allowing open direction which could potentially be used for phishing** #34

```
Can folks please review the impact description and related metadata in the
draft OSSA-2021-002 linked above? I've left the CVE blank for now since
I'm waiting for Nick to say what number he assigned.
```

Nick Tait (nickthetait) wrote on 2021-07-27: #35

```
CVE-2021-3654 https://access.redhat.com/security/cve/CVE-2021-3654
```

Nick Tait (nickthetait) wrote on 2021-07-27: #36

```
And cheers to the trio at Monash for reporting. Thanks!
```

Jeremy Stanley (fungi) wrote on 2021-07-28: **Re: Open Redirect in noVNC proxy (CVE-2021-3654)** #37

```
The draft advisory has been updated with the CVE (thanks again, Nick!) and
a proposed publication date of tomorrow, so if folks could please review
https://review.opendev.org/802590 that will help a ton.
```

```
summary:- novnc allowing open direction which could potentially be used for
        - phishing
        + Open Redirect in noVNC proxy (CVE-2021-3654)
Changed in ossa:
 status:In Progress → Fix Committed
```

OpenStack Infra (hudson-openstack) wrote on 2021-07-29: **Fix merged to ossa (master)** #38

```
Reviewed: https://review.opendev.org/c/openstack/ossa/+/802590
Committed: https://opendev.org/openstack/ossa/commit/08f2c78ccf3688a
d2ed44d0c2239742ea1693cdb
Submitter: "Zuul (22348)"
Branch: master

commit 08f2c78ccf3688ad2ed44d0c2239742ea1693cdb
Author: Jeremy Stanley <email address hidden>
Date: Tue Jul 27 17:44:41 2021 +0000

    Add OSSA-2021-002 (CVE-2021-3654)

    Change-Id: I1574738a9aa047314c9b933f8bbe032d346cd2d7
    Closes-Bug: #1927677
```

```
Changed in ossa:
status:Fix Committed → Fix Released
```

Jeremy Stanley (fungi) on 2021-07-29

```
summary:- Open Redirect in noVNC proxy (CVE-2021-3654)
        + [OSSA-2021-002]Open Redirect in noVNC proxy (CVE-2021-3654)
summary:- [OSSA-2021-002]Open Redirect in noVNC proxy (CVE-2021-3654)
        + [OSSA-2021-002] Open Redirect in noVNC proxy (CVE-2021-3654)
```

OpenStack Infra (hudson-openstack) wrote on 2021-07-29: **Fix proposed to nova (stable/stein)** #39

```
Fix proposed to branch: stable/stein
Review: https://review.opendev.org/c/openstack/nova/+/802935
```

OpenStack Infra (hudson-openstack) wrote on 2021-07-31: **Related fix proposed to nova (master)** #40

Related fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/nova/+/803091

melanie witt (melwitt) wrote on 2021-07-31: #41

This ^ is just me updating the unit test coverage to work with Python < 3.6 for the courtesy stable/train and stable/stein patches. It's also a general improvement of the unit test to do less mocking.

OpenStack Infra (hudson-openstack) wrote on 2021-07-31: **Related fix proposed to nova (stable/wallaby)** #42

Related fix proposed to branch: stable/wallaby
Review: https://review.opendev.org/c/openstack/nova/+/803092

OpenStack Infra (hudson-openstack) wrote on 2021-07-31: **Related fix proposed to nova (stable/victoria)** #43

Related fix proposed to branch: stable/victoria
Review: https://review.opendev.org/c/openstack/nova/+/803093

OpenStack Infra (hudson-openstack) wrote on 2021-07-31: **Related fix proposed to nova (stable/ussuri)** #44

Related fix proposed to branch: stable/ussuri
Review: https://review.opendev.org/c/openstack/nova/+/803094

OpenStack Infra (hudson-openstack) wrote on 2021-08-02: **Fix proposed to nova (stable/rocky)** #45

Fix proposed to branch: stable/rocky
Review: https://review.opendev.org/c/openstack/nova/+/803182

Matteo Pozza (matteopozza) wrote on 2021-08-23: #46

Hi,

me and my colleagues were noticing that the patch protects against URLs starting with two slashes, with four slashes, and with more than four slashes. Nevertheless, the patch does not seem to work in case the URL starts with three slashes, e.g.:

http://vncproxy.my.domain.com//example.com/%2F..

We believe that the reason behind this behaviour is the changes that the URL undergoes when it is split and then unsplit. More specifically:

```
>>> urlparse.urlunsplit(urlparse.urlsplit('//example.com/%2F..'))
'//example.com/%2F..'
>>> urlparse.urlunsplit(urlparse.urlsplit('///example.com/%2F..'))
'/example.com/%2F..'
>>> urlparse.urlunsplit(urlparse.urlsplit('////example.com/%2F..'))
'//example.com/%2F..'
```

The first and the last case will be captured by the test introduced by the patch, while the middle case will be sent to the parent class method. This can be observed with both Python 3 and Python 2.

We think that the unsplitting of the url in the patch could be avoided. In the case of Python 3, the reason for which the method is used is to add a final slash to the "path" part of the URL, but this is nevertheless not needed for our purposes (if the URL passes the validity check performed here, the splitting and unsplitting of the URL will be anyway done by the parent class method). Moreover, using the output of the urlsplit + urlunsplit methods causes the aforementioned issue.

I will soon attach a proposal for a Python 2 and a Python 3 patch. Their checks on the URL are slightly different because they mimic the checks that are done by the parent class method in order to identify a redirection case (SimpleHTTPRequestHandler.send_head defined in SimpleHttpServer.py for Python2 and in http/server.py for Python 3).
Please let me know if you are able to reproduce the same issue in your setup and what you think about this.

Matteo Pozza (matteopozza) wrote on 2021-08-23: #47

python2.patch (1.2 KiB, text/plain)

This is a proposal for Python 2.

Matteo Pozza (matteopozza) wrote on 2021-08-23: #48

python3.patch (1009 bytes, text/plain)

This is a proposal for Python 3.

OpenStack Infra (hudson-openstack) wrote on 2021-08-23: **Fix proposed to nova (master)** #49

Fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/nova/+/805654

Balazs Gibizer (balazs-gibizer) wrote on 2021-08-24: #50

It is confirmed that the original fix was incomplete. A new fix is being merged to master https://review.opendev.org/c/openstack/nova/+/805654 (and then backported)

Changed in nova:
status:Fix Released → In Progress

OpenStack Infra (hudson-openstack) wrote on 2021-08-24: **Fix merged to nova (master)** #51

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/805654
Committed: https://opendev.org/openstack/nova/commit/6fbd0b758dcac71
323f3be179b1a9d1c17a4acc5
Submitter: "Zuul (22348)"
Branch: master

commit 6fbd0b758dcac71323f3be179b1a9d1c17a4acc5
Author: Sean Mooney <email address hidden>
Date: Mon Aug 23 15:37:48 2021 +0100

    address open redirect with 3 forward slashes

    Ie36401c782f023d1d5f2623732619105dc2cfa24 was intended
    to address OSSA-2021-002 (CVE-2021-3654) however after its
    release it was discovered that the fix only worked
    for urls with 2 leading slashes or more then 4.

    This change adresses the missing edgecase for 3 leading slashes
    and also maintian support for rejecting 2+.

    Change-Id: I95f68be76330ff09e5eabb5ef8dd9a18f5547866
    co-authored-by: Matteo Pozza
    Closes-Bug: #1927677
```

Changed in nova:
status: In Progress → Fix Released

Jeremy Stanley (fungi) wrote on 2021-08-24: #52

```
I've switched the security advisory task back to incomplete for now, while
the vulnerability managers debate whether this requires errata publication
or a completely new advisory.
```

Changed in ossa:
status: Fix Released → Incomplete
importance: Medium → Undecided
assignee: Jeremy Stanley (fungi) → nobody

OpenStack Infra (hudson-openstack) wrote on 2021-08-24: **Fix proposed to nova (stable/wallaby)** #53

```
Fix proposed to branch: stable/wallaby
Review: https://review.opendev.org/c/openstack/nova/+/805818
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-28: **Fix merged to nova (stable/wallaby)** #54

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/805818
Committed: https://opendev.org/openstack/nova/commit/47dad4836a26292
e9d34e516e1525ecf00be127c
Submitter: "Zuul (22348)"
Branch: stable/wallaby

commit 47dad4836a26292e9d34e516e1525ecf00be127c
Author: Sean Mooney <email address hidden>
Date: Mon Aug 23 15:37:48 2021 +0100

    address open redirect with 3 forward slashes

    Ie36401c782f023d1d5f2623732619105dc2cfa24 was intended
    to address OSSA-2021-002 (CVE-2021-3654) however after its
    release it was discovered that the fix only worked
    for urls with 2 leading slashes or more then 4.

    This change adresses the missing edgecase for 3 leading slashes
    and also maintian support for rejecting 2+.

    Change-Id: I95f68be76330ff09e5eabb5ef8dd9a18f5547866
    co-authored-by: Matteo Pozza
    Closes-Bug: #1927677
    (cherry picked from commit 6fbd0b758dcac71323f3be179b1a9d1c17a4acc5)
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-30: **Related fix merged to nova (master)** #55

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/803091
Committed: https://opendev.org/openstack/nova/commit/214cabe6848a1fd
b4f5941d994c6cc11107fc4af
Submitter: "Zuul (22348)"
Branch: master

commit 214cabe6848a1fdb4f5941d994c6cc11107fc4af
Author: melanie witt <email address hidden>
Date: Sat Jul 31 00:30:16 2021 +0000

    Reduce mocking in test_reject_open_redirect for compat

    This is a followup for change Ie36401c782f023d1d5f2623732619
105dc2cfa24
    to reduce mocking in the unit test coverage for it.

    While backporting the bug fix, it was found to be incompatible with
    earlier versions of Python < 3.6 due to a difference in internal
    implementation [1].

    This reduces the mocking in the unit test to be more agnostic to the
    internals of the StreamRequestHandler (ancestor of
    SimpleHTTPRequestHandler) and work across Python versions >= 2.7.

    Related-Bug: #1927677

    [1] https://github.com/python/cpython/commit/34eeed42901666f
ce099947f93dfdfc05411f286

    Change-Id: I546d376869a992601b443fb95acf1034da2a8f36
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-30: **Fix proposed to nova (stable/victoria)** #56

```
Fix proposed to branch: stable/victoria
Review: https://review.opendev.org/c/openstack/nova/+/806626
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-30: **Fix proposed to nova (stable/ussuri)** #57

```
Fix proposed to branch: stable/ussuri
Review: https://review.opendev.org/c/openstack/nova/+/806628
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-30: **Fix proposed to nova (stable/train)** #58

```
Fix proposed to branch: stable/train
Review: https://review.opendev.org/c/openstack/nova/+/806629
```

OpenStack Infra (hudson-openstack) wrote on 2021-08-31: **Related fix merged to nova (stable/wallaby)** #59

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/803092
Committed: https://opendev.org/openstack/nova/commit/9c2f29783734cb5
f9cb05a08d328c10e1d16c4f1
Submitter: "Zuul (22348)"
Branch: stable/wallaby

commit 9c2f29783734cb5f9cb05a08d328c10e1d16c4f1
Author: melanie witt <email address hidden>
Date: Sat Jul 31 00:30:16 2021 +0000

    Reduce mocking in test_reject_open_redirect for compat

    This is a followup for change Ie36401c782f023d1d5f2623732619
105dc2cfa24
    to reduce mocking in the unit test coverage for it.

    While backporting the bug fix, it was found to be incompatible with
    earlier versions of Python < 3.6 due to a difference in internal
    implementation [1].

    This reduces the mocking in the unit test to be more agnostic to the
    internals of the StreamRequestHandler (ancestor of
    SimpleHTTPRequestHandler) and work across Python versions >= 2.7.

    Related-Bug: #1927677

    [1] https://github.com/python/cpython/commit/34eeed42901666f
ce099947f93dfdfc05411f286

    Change-Id: I546d376869a992601b443fb95acf1034da2a8f36
    (cherry picked from commit 214cabe6848a1fdb4f5941d994c6cc11107fc4af)
```

tags:added: in-stable-wallaby

OpenStack Infra (hudson-openstack) wrote on 2021-09-01: **Related fix merged to nova (stable/victoria)** #60

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/803093
Committed: https://opendev.org/openstack/nova/commit/94e265f3ca615aa
18de0081a76975019997b8709
Submitter: "Zuul (22348)"
Branch: stable/victoria

commit 94e265f3ca615aa18de0081a76975019997b8709
Author: melanie witt <email address hidden>
Date: Sat Jul 31 00:30:16 2021 +0000

    Reduce mocking in test_reject_open_redirect for compat

    This is a followup for change Ie36401c782f023d1d5f2623732619
105dc2cfa24
    to reduce mocking in the unit test coverage for it.

    While backporting the bug fix, it was found to be incompatible with
    earlier versions of Python < 3.6 due to a difference in internal
    implementation [1].

    This reduces the mocking in the unit test to be more agnostic to the
    internals of the StreamRequestHandler (ancestor of
    SimpleHTTPRequestHandler) and work across Python versions >= 2.7.

    Related-Bug: #1927677

    [1] https://github.com/python/cpython/commit/34eeed42901666f
ce099947f93dfdfc05411f286

    Change-Id: I546d376869a992601b443fb95acf1034da2a8f36
    (cherry picked from commit 214cabe6848a1fdb4f5941d994c6cc11107fc4af)
    (cherry picked from commit 9c2f29783734cb5f9cb05a08d328c10e1d16c4f1)
```

tags:added: in-stable-victoria

OpenStack Infra (hudson-openstack) wrote on 2021-09-14: **Related fix merged to nova (stable/ussuri)** #61

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/803094
Committed: https://opendev.org/openstack/nova/commit/d43b88a33407b12
53e7bce70f720a44f7688141f
Submitter: "Zuul (22348)"
Branch: stable/ussuri

commit d43b88a33407b1253e7bce70f720a44f7688141f
Author: melanie witt <email address hidden>
Date: Sat Jul 31 00:30:16 2021 +0000

    Reduce mocking in test_reject_open_redirect for compat

    This is a followup for change Ie36401c782f023d1d5f2623732619
105dc2cfa24
    to reduce mocking in the unit test coverage for it.

    While backporting the bug fix, it was found to be incompatible with
    earlier versions of Python < 3.6 due to a difference in internal
    implementation [1].

    This reduces the mocking in the unit test to be more agnostic to the
    internals of the StreamRequestHandler (ancestor of
    SimpleHTTPRequestHandler) and work across Python versions >= 2.7.

    Related-Bug: #1927677

    [1] https://github.com/python/cpython/commit/34eeed42901666f
ce099947f93dfdfc05411f286

    Change-Id: I546d376869a992601b443fb95acf1034da2a8f36
    (cherry picked from commit 214cabe6848a1fdb4f5941d994c6cc11107fc4af)
    (cherry picked from commit 9c2f29783734cb5f9cb05a08d328c10e1d16c4f1)
    (cherry picked from commit 94e265f3ca615aa18de0081a76975019997b8709)
```

tags:added: in-stable-ussuri

OpenStack Infra (hudson-openstack) wrote on 2021-09-16: **Fix merged to nova (stable/victoria)** #62

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/806626
Committed: https://opendev.org/openstack/nova/commit/9588cdbfd4649ea
53d60303f2d10c5d62a070a07
Submitter: "Zuul (22348)"
Branch: stable/victoria

commit 9588cdbfd4649ea53d60303f2d10c5d62a070a07
Author: Sean Mooney <email address hidden>
Date: Mon Aug 23 15:37:48 2021 +0100

    address open redirect with 3 forward slashes

    Ie36401c782f023d1d5f2623732619105dc2cfa24 was intended
    to address OSSA-2021-002 (CVE-2021-3654) however after its
    release it was discovered that the fix only worked
    for urls with 2 leading slashes or more then 4.

    This change adresses the missing edgecase for 3 leading slashes
    and also maintian support for rejecting 2+.

    Conflicts:
      nova/tests/unit/console/test_websocketproxy.py

    NOTE: conflict is due to I58b0382c86d4ef798572edb63d311e0e3e6937bb
    is missing in Victoria and Ie36401c782f023d1d5f2623732619105dc2cfa24
    backport contained conflicts and methods order was swapped.

    Change-Id: I95f68be76330ff09e5eabb5ef8dd9a18f5547866
    co-authored-by: Matteo Pozza
    Closes-Bug: #1927677
    (cherry picked from commit 6fbd0b758dcac71323f3be179b1a9d1c17a4acc5)
    (cherry picked from commit 47dad4836a26292e9d34e516e1525ecf00be127c)
```

OpenStack Infra (hudson-openstack) wrote on 2021-09-17: **Fix included in openstack/nova 24.0.0.0rc1** #63

This issue was fixed in the openstack/nova 24.0.0.0rc1 release candidate.

Jeremy Stanley (fungi) wrote on 2021-09-24: #65

Note that we're still waiting for https://review.opendev.org/806628 (stable/ussuri) to merge prior to issuing errata, but its merging is held up by discussions of whether to fix or discontinue running lower bounds testing for dependencies on that branch.

melanie witt (melwitt) wrote on 2021-09-24: #66

We have actually been rechecking this change to make the l-c job non-voting on stable/ussuri:

https://review.opendev.org/c/openstack/nova/+/809955

But it has run into failure after unrelated failure in the gate. I have been copy pasting the various errors with every recheck.

OpenStack Infra (hudson-openstack) wrote on 2021-09-26: **Fix merged to nova (stable/ussuri)** #67

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/806628
Committed: https://opendev.org/openstack/nova/commit/0997043f459ac61
6b594363b5b253bd0ae6ed9eb
Submitter: "Zuul (22348)"
Branch: stable/ussuri

commit 0997043f459ac616b594363b5b253bd0ae6ed9eb
Author: Sean Mooney <email address hidden>
Date: Mon Aug 23 15:37:48 2021 +0100

    address open redirect with 3 forward slashes

    Ie36401c782f023d1d5f2623732619105dc2cfa24 was intended
    to address OSSA-2021-002 (CVE-2021-3654) however after its
    release it was discovered that the fix only worked
    for urls with 2 leading slashes or more then 4.

    This change adresses the missing edgecase for 3 leading slashes
    and also maintian support for rejecting 2+.

    Change-Id: I95f68be76330ff09e5eabb5ef8dd9a18f5547866
    co-authored-by: Matteo Pozza
    Closes-Bug: #1927677
    (cherry picked from commit 6fbd0b758dcac71323f3be179b1a9d1c17a4acc5)
    (cherry picked from commit 47dad4836a26292e9d34e516e1525ecf00be127c)
    (cherry picked from commit 9588cdbfd4649ea53d60303f2d10c5d62a070a07)
```

OpenStack Infra (hudson-openstack) wrote on 2021-09-27: **Fix proposed to ossa (master)** #68

Fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/ossa/+/811181

Changed in ossa:
status:Incomplete → In Progress

OpenStack Infra (hudson-openstack) wrote on 2021-09-27: **Fix merged to ossa (master)** #69

```
Reviewed: https://review.opendev.org/c/openstack/ossa/+/811181
Committed: https://opendev.org/openstack/ossa/commit/51a1bf0699128c8
ddcb7567347cee69492601091
Submitter: "Zuul (22348)"
Branch: master

commit 51a1bf0699128c8ddcb7567347cee69492601091
Author: Jeremy Stanley <email address hidden>
Date: Mon Sep 27 15:02:06 2021 +0000
```

```
    Errata 1 for OSSA-2021-002

    Change-Id: Iaeb40574176ae62542a0c17e94917e654d38317d
    Closes-Bug: #1927677
```

Changed in ossa:
status: In Progress → Fix Released

Jeremy Stanley (fungi) wrote on 2021-09-27: #70

OSSA-2021-002 errata 1 has been published and distributed to usual mailing lists.

OpenStack Infra (hudson-openstack) wrote on 2021-10-07: **Fix included in openstack/nova 22.3.0** #71

This issue was fixed in the openstack/nova 22.3.0 release.

OpenStack Infra (hudson-openstack) wrote on 2021-10-07: **Fix included in openstack/nova 23.1.0** #73

This issue was fixed in the openstack/nova 23.1.0 release.

OpenStack Infra (hudson-openstack) wrote on 2021-10-07: **Fix included in openstack/nova 21.2.3** #74

This issue was fixed in the openstack/nova 21.2.3 release.

OpenStack Infra (hudson-openstack) wrote on 2021-10-28: **Fix merged to nova (stable/train)** #76

Download full text (3.2 KiB)

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/791807
Committed: https://opendev.org/openstack/nova/commit/04d48527b62a35d
912f93bc75613a6cca606df66
Submitter: "Zuul (22348)"
Branch: stable/train

commit 04d48527b62a35d912f93bc75613a6cca606df66
Author: melanie witt <email address hidden>
Date: Thu May 13 05:43:42 2021 +0000

    Reject open redirection in the console proxy

    NOTE(melwitt): This is the combination of two commits, the bug fix and
    a followup change to the unit test to enable it also run on
    Python < 3.6.

    Our console proxies (novnc, serial, spice) run in a websockify server
    whose request handler inherits from the python standard
    SimpleHTTPRequestHandler. There is a known issue [1] in the
    SimpleHTTPRequestHandler which allows open redirects by way of URLs
    in the following format:

      http://vncproxy.my.domain.com//example.com/%2F..

    which if visited, will redirect a user to example.com.

    We can intercept a request and reject requests that pass a redirection
    URL beginning with "//" by implementing the
    SimpleHTTPRequestHandler.send_head() method containing the
    vulnerability to reject such requests with a 400 Bad Request.

    This code is copied from a patch suggested in one of the issue
comments
    [2].

    Closes-Bug: #1927677

    [1] https://bugs.python.org/issue32084
    [2] https://bugs.python.org/issue32084#msg306545

    Conflicts:
        nova/tests/unit/console/test_websocketproxy.py

    NOTE(melwitt): The conflict is because change
    I23ac1cc79482d0fabb359486a4b934463854cae5 (Allow TLS ciphers/protocols
    to be configurable for console proxies) is not in Train.

    NOTE(melwitt): The difference from the cherry picked change:
    HTTPStatus.BAD_REQUEST => 400 is due to the fact that HTTPStatus does
    not exist in Python 2.7.

    Reduce mocking in test_reject_open_redirect for compat

    This is a followup for change Ie36401c782f023d1d5f2623732619
105dc2cfa24
    to reduce mocking in the unit test coverage for it.

    While backporting the bug fix, it was found to be incompatible with
    earlier versions of Python < 3.6 due to a difference in internal
    implementation [1].

    This reduces the mocking in the unit test to be more agnostic to the
    internals of the StreamRequestHandler (ancestor of
    SimpleHTTPRequestHandler) and work across Python versions >= 2.7.

    Related-Bug: #1927677

    [1] https://github.com/python/cpython/commit/34eeed42901666f
ce099947f93dfdfc05411f286

    Change-Id: I546d376869a992601b443fb95acf1034da2a8f36
    (cherry picked from commit 214cabe6848a1fdb4f5941d994c6cc11107fc4af)
    (cherry picked from commit 9c2f29783734cb5f9cb05a08d328c10e1d16c4f1)
    (cherry picked from commit 94e265f3ca615aa18de0081a76975019997b8709)
    (cherry picked from commit d43b88a33407b1253e7bce70f720a44f7688141f)

    Change-Id: Ie36401c782f023d1d5f2623732619105dc2cfa24
    (cherry picked from commit 781612b33282ed298f742c85dab58a075c8b793e)
    (cherry picked from commit 470925614223c8dd9b1233f54f5a96c02b2d4f70)
    (cherry picked from commit 6b70350bdcf5...
```

Read more...

OpenStack Infra (hudson-openstack) wrote on 2021-11-01: #77

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/806629
Committed: https://opendev.org/openstack/nova/commit/8906552cfc2525a
44251d4cf313ece61e57251eb
Submitter: "Zuul (22348)"
Branch: stable/train

commit 8906552cfc2525a44251d4cf313ece61e57251eb
Author: Sean Mooney <email address hidden>
Date: Mon Aug 23 15:37:48 2021 +0100

    address open redirect with 3 forward slashes

    Ie36401c782f023d1d5f2623732619105dc2cfa24 was intended
    to address OSSA-2021-002 (CVE-2021-3654) however after its
    release it was discovered that the fix only worked
    for urls with 2 leading slashes or more then 4.

    This change adresses the missing edgecase for 3 leading slashes
    and also maintian support for rejecting 2+.

    Conflicts:
      nova/console/websocketproxy.py
      nova/tests/unit/console/test_websocketproxy.py

    NOTE(melwitt): The conflict and difference in websocketproxy.py from
    the cherry picked change: HTTPStatus.BAD_REQUEST => 400 is due to the
    fact that HTTPStatus does not exist in Python 2.7. The conflict in
    test_websocketproxy.py is because change
    I23ac1cc79482d0fabb359486a4b934463854cae5 (Allow TLS ciphers/protocols
    to be configurable for console proxies) is not in Train. The
difference
    in test_websocketproxy.py from the cherry picked change is due to a
    difference in internal implementation [1] in Python < 3.6. See change
    I546d376869a992601b443fb95acf1034da2a8f36 for reference.

    [1] https://github.com/python/cpython/commit/34eeed42901666f
ce099947f93dfdfc05411f286

    Change-Id: I95f68be76330ff09e5eabb5ef8dd9a18f5547866
    co-authored-by: Matteo Pozza
    Closes-Bug: #1927677
    (cherry picked from commit 6fbd0b758dcac71323f3be179b1a9d1c17a4acc5)
    (cherry picked from commit 47dad4836a26292e9d34e516e1525ecf00be127c)
    (cherry picked from commit 9588cdbfd4649ea53d60303f2d10c5d62a070a07)
    (cherry picked from commit 0997043f459ac616b594363b5b253bd0ae6ed9eb)
```

OpenStack Infra (hudson-openstack) wrote on 2021-11-08: **Fix proposed to nova (stable/stein)** #78

```
Fix proposed to branch: stable/stein
Review: https://review.opendev.org/c/openstack/nova/+/817037
```

OpenStack Infra (hudson-openstack) wrote on 2022-08-17: **Related fix proposed to nova (master)** #79

```
Related fix proposed to branch: master
Review: https://review.opendev.org/c/openstack/nova/+/853379
```

OpenStack Infra (hudson-openstack) wrote on 2022-08-30: **Related fix merged to nova (master)** #80

```
Reviewed: https://review.opendev.org/c/openstack/nova/+/853379
Committed: https://opendev.org/openstack/nova/commit/15769b883ed4a86
d62b141ea30d3f1590565d8e0
Submitter: "Zuul (22348)"
Branch: master

commit 15769b883ed4a86d62b141ea30d3f1590565d8e0
Author: melanie witt <email address hidden>
Date: Tue Aug 16 06:49:53 2022 +0000

    Adapt websocketproxy tests for SimpleHTTPServer fix

    In response to bug 1927677 we added a workaround to
    NovaProxyRequestHandler to respond with a 400 Bad Request if an open
    redirect is attempted:

      Ie36401c782f023d1d5f2623732619105dc2cfa24
      I95f68be76330ff09e5eabb5ef8dd9a18f5547866

    Recently in python 3.10.6, a fix has landed in cpython to respond with
    a 301 Moved Permanently to a sanitized URL that has had extra leading
    '/' characters removed.

    This breaks our existing unit tests which assume a 400 Bad Request as
    the only expected response.

    This adds handling of a 301 Moved Permanently response and asserts
that
    the redirect location is the expected sanitized URL. Doing this
instead
    of checking for a given python version will enable the tests to
continue
    to work if and when the cpython fix gets backported to older python
    versions.

    While updating the tests, the opportunity was taken to commonize the
    code of two unit tests that were nearly identical.

    Related-Bug: #1927677
    Closes-Bug: #1986545

    Change-Id: I27441d15cc6fa2ff7715ba15aa900961aadbf54a
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-11: **Change abandoned on nova (stable/rocky)** #81

```
Change abandoned by "Elod Illes <email address hidden>" on branch:
stable/rocky
Review: https://review.opendev.org/c/openstack/nova/+/803182
Reason: This branch transitioned to End of Life for this project, open
patches needs to be closed to be able to delete the branch.
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-11: **Change abandoned on nova (stable/stein)** #82

```
Change abandoned by "Elod Illes <email address hidden>" on branch:
stable/stein
Review: https://review.opendev.org/c/openstack/nova/+/817037
Reason: This branch transitioned to End of Life for this project, open
patches needs to be closed to be able to delete the branch.
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-11: #83

```
Change abandoned by "Elod Illes <email address hidden>" on branch:
stable/stein
Review: https://review.opendev.org/c/openstack/nova/+/802935
Reason: This branch transitioned to End of Life for this project, open
patches needs to be closed to be able to delete the branch.
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-30: **Related fix proposed to nova (stable/yoga)** #84

```
Related fix proposed to branch: stable/yoga
Review: https://review.opendev.org/c/openstack/nova/+/866192
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-30: **Related fix proposed to nova (stable/xena)** #85

```
Related fix proposed to branch: stable/xena
Review: https://review.opendev.org/c/openstack/nova/+/866193
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-30: **Related fix proposed to nova (stable/wallaby)** #86

```
Related fix proposed to branch: stable/wallaby
Review: https://review.opendev.org/c/openstack/nova/+/866194
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-30: **Related fix proposed to nova (stable/victoria)** #87

```
Related fix proposed to branch: stable/victoria
Review: https://review.opendev.org/c/openstack/nova/+/866195
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-30: **Related fix proposed to nova (stable/ussuri)** #88

```
Related fix proposed to branch: stable/ussuri
Review: https://review.opendev.org/c/openstack/nova/+/866196
```

OpenStack Infra (hudson-openstack) wrote on 2022-11-30: **Related fix proposed to nova (stable/train)** #89

```
Related fix proposed to branch: stable/train
Review: https://review.opendev.org/c/openstack/nova/+/866201
```

See full activity log

To post a comment you must log in.