



Immersive-Labs-Sec / nimbuspwn Public

☆ Star 22

main



Code ▼

 README.md



nimbuspwn-sigma.yml



nimbuspwn.py



# README



por

cve-2022-29799

cve-2022-29800

nimbuspwn



## Readme



## Activity



## Custom properties



22 stars



0 watching



7 forks

Report repository

No releases published

No packages published

## Contributors 3

naomshi Naomi

Page 1 of 3

This vulnerability is generally not present in pure `systemd-networkd` based systems, since in that case, the legitimate `systemd-networkd` process will be holding the required D-Bus name. However, it is present where attempts have been made to disable `systemd-networkd`, for example using scripts such as <https://gist.github.com/polrus/772618cfead9c1b63b246584024d7765>, which enables `NetworkManager` for Ubuntu Server installs.

## Commands

```
sudo apt update
sudo apt -y install network-manager
sudo nano /etc/cloud/cloud.cfg.d/99-disable-netplan
Add content: "network: {config: disabled}" and :
sudo nano /etc/netplan/50-cloud-init.yaml
Add "renderer: NetworkManager" to "network:" block
sudo netplan generate
sudo netplan apply
sudo systemctl enable NetworkManager.service
sudo systemctl restart NetworkManager.service
sudo systemctl disable systemd-networkd
```



**mpettitt** Matthew Pettitt



**kevthehermit** TheHermit

## Languages

● Python 100.0%

## Detection

To aid detection of this specific poc we have released a sigma rule. It should be noted that this sigma rule is specific to our poc code and may not detect all possible exploit attempts.

## License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or

sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN