

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing


🔍


Sign in

Sign up

📁 Immersive-Labs-Sec / nimbuspwn Public

🔔 Notifications

 Fork 7

 Star 22

<> Code

🕒 Issues

🔗 Pull requests


🎬 Actions


📁 Projects

🛡 Security

📈 Insights

🔗 main ▾







🔍




Go to file


<> Code ▾

 **mpettitt** Update README.md ...

b364cfe · 2 years ago

 12 Commits

 README.md	Update README.md	2 years ago
 nimbuspwn-sigma.yml	Add Sigma Rule for nimbuspwn	2 years ago
 nimbuspwn.py	rename script	2 years ago

 README

☰

nimbuspwn

This is a PoC for Nimbuspwn, as originally described in <https://www.microsoft.com/security/blog/2022/04/26/microsoft-finds-new-elevation-of-privilege-linux-vulnerability-nimbuspwn/>

It runs reliably on Ubuntu Desktop installs, but does not run by default on Ubuntu Server installs. It is possible to configure a server install to be vulnerable, although this is not expected to be a common configuration.

Making an AWS Instance Vulnerable

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-network-config.cfg
Add content: "network: {config: disabled}" and save
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
```

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.

About


This is a PoC for Nimbuspwn, a Linux privilege escalation issue identified by Microsoft


poc


cve-2022-29799


cve-2022-29800


nimbuspwn


 Readme

 Activity

 Custom properties

 22 stars

 0 watching

 7 forks

Report repository

Releases


No releases published


Packages


No packages published

Contributors

3

 **naomshi** Naomi

 **mpettitt** Matthew Pettitt

 **kevthehermit** TheHermit

Languages

● Python 100.0%

Page 1 of 2

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 THE SOFTWARE.

