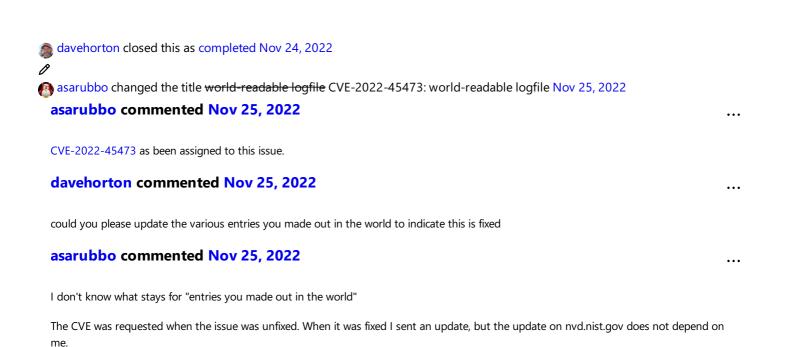
```
☐ drachtio / drachtio-server Public
     Code
      Issues 66
           Pull requests 4
       Actions
       Projects
    Wiki
       Security
       Insights
CVE-2022-45473: world-readable logfile #241
                                                                                                                      New issue
                                                                                                               Jump to bottom

    Closed

asarubbo opened this issue Nov 18, 2022 · 4 comments
  asarubbo commented Nov 18, 2022
  Hello,
  when drachtio-server starts, creates /var/log/drachtio with mode 777
  This leads to a disclosure because a local user can retrieve sensitive data (like IP and so on).
  Here is the details:
    drachtio1 ~ # systemctl stop drachtio
    drachtio1 ~ # rm -fr /var/log/drachtio
    drachtio1 ~ # systemctl start drachtio
    drachtio1 ~ # ls -la /var/log/drachtio/
    total 12
    drwxrwxrwx 3 root root 4096 Nov 18 16:01 .
    drwxr-xr-x 15 root root 4096 Nov 18 16:01 ..
    drwxrwxrwx 2 root root 4096 Nov 18 16:01 archive
    -rw-rw-rw- 1 root root
                              0 Nov 18 16:01 drachtio.log
  To fix this issue, /var/log/drachtio should be created with mode 770
davehorton added a commit that referenced this issue Nov 23, 2022
make drachtio log file not globally readable (#241)
                                                                                                                        f791a93
\mathbb{C}^{2}
davehorton added a commit that referenced this issue Nov 24, 2022
add --globally-readable-logs as part of #241
                                                                                                                        4f3530f
  davehorton commented Nov 24, 2022
```

0

fixed in v0.8.19-rc12



Sign up for free

to join this conversation on GitHub. Already have an account? Sign in to comment

Assignees No one assigned Labels None yet Projects None yet Milestone No milestone Development No branches or pull requests 2 participants © 2022 GitHub, Inc.



Privacy

Security

Status

Docs

Contact GitHub

Pricing

API

Training

Blog

About