

[New issue](#)[Jump to bottom](#)

CVE-2022-45473: world-readable logfile #241

🔒 Closed asarubbo opened this issue 8 days ago · 4 comments

asarubbo commented 8 days ago

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 3 days ago

make drachtio log file not globally readable (#241)

✗ f791a93 davehorton added a commit that referenced this issue 2 days ago

add --globally-readable-logs as part of #241

✗ 4f3530f

davehorton commented 2 days ago

Collaborator

fixed in v0.8.19-rc12



davehorton closed this as completed 2 days ago



asarubbo changed the title ~~world-readable logfile~~ **CVE-2022-45473: world-readable logfile**
19 hours ago

asarubbo commented 19 hours ago

Author

[CVE-2022-45473](#) as been assigned to this issue.

davehorton commented 18 hours ago

Collaborator

could you please update the various entries you made out in the world to indicate this is fixed

asarubbo commented 18 hours ago

Author

I don't know what stays for "entries you made out in the world"

The CVE was requested when the issue was unfixed. When it was fixed I sent an update, but the update on [nvd.nist.gov](#) does not depend on me.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

no branches or pull requests

2 participants

