New issue

Jump to bottom

[Bug] Wrong permissions in grafana package for grafana.db #8283

Closed **austinbutler** opened this issue on May 3, 2017 · 8 comments · Fixed by #26339

Assignees	
Labels	area/backend/db area/security help wanted
Projects	Backend Platform Squad
Milestone	7.2.0-beta1

austinbutler commented on May 3, 2017

It looks like in #2126 there were plans to lock down the sqlite DB to 0600. While grafana.ini did get locked down, the DB did not. Unless this is no longer believed to be necessary I could try to send a PR.

- What Grafana version are you using? 4.2.0
- What datasource are you using? InfluxDB
- What OS are you running grafana on? CentOS 7.3.1611
- What did you do? Logged into grafana.db as a regular user
- What was the expected result? Permission denied
- What happened instead? Logged in without issue, able to query salt and password for users

```
[vagrant@monitoring ~]$ less /etc/grafana/grafana.ini
/etc/grafana/grafana.ini: Permission denied
[vagrant@monitoring ~]$ sqlite3 /var/lib/grafana/grafana.db
SQLite version 3.7.17 2013-05-20 00:56:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> select salt, password from user;
SALT|PW
[vagrant@noc-monitoring ~]$ sudo yum info grafana
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.chi.host-engine.com
 * extras: mirror.sigmanet.com
 * updates: mirror.sigmanet.com
Installed Packages
Name        : grafana
Arch        : x86_64
Version     : 4.2.0
Release     : 1
Size        : 128 M
Repo        : installed
From repo   : grafana
Summary     : Grafana
URL         : https://grafana.com
License     : "Apache 2.0"
Description : Grafana
```

torkelo added area/security area/backend/db help wanted labels on May 4, 2017

torkelo commented on May 4, 2017 Member

I think Grafana needs to change the file permission after the db file is created (first startup). It is created by sqlite though so has to happen after db is initialized.

andreasgerstmayr commented on Apr 28, 2020 Contributor

It's possible to create an empty `grafana.db` file with the correct permissions - sqlite won't complain and will use this file.

Alternatively the permissions of the `/var/lib/grafana` directory could be set to `750`. Does it need to be world-readable?

justin007755 commented on May 5, 2020

Yes, the permission of the /var/lib/grafana directory should be updated as well. Is there any plan to fix this potential security issue or users have to run some manual mitigations by themselves?

👍 1

torkelo commented on May 6, 2020 Member

How did you install Grafana? What package?

aknuds1 self-assigned this on Jul 8, 2020

aknuds1 added this to **To do** in **Backend Platform Squad** on Jul 8, 2020

aknuds1 mentioned this issue on Jul 14, 2020

grafana.db should not be mode 755 #26313

Closed

wz2b commented on Jul 14, 2020

> Yes, the permission of the /var/lib/grafana directory should be updated as well. Is there any plan to fix this potential security issue or users have to run some manual mitigations by themselves?

From the FHS standard:

> This hierarchy holds state information pertaining to an application or the system. State information is data
> that programs modify while they run, and that pertains to one specific host. Users must never need to
> modify files in /var/lib to configure a package's operation, and the specific file hierarchy used to store
> the data must not be exposed to regular users.
>
> State information is generally used to preserve the condition of an application (or a group of interrelated applications) between invocations and between different instances of the same application. State
> information should generally remain valid after a reboot, should not be logging output, and should not
> be spooled data.

So yeah, I agree that permissions on both grafana.db (after creation) and the directory itself could be closed. I think setting 750 on the directory makes sense, but grafana.db probably needs to be 600. This might not really matter as I doubt anybody puts themselves in the 'grafana' group but who knows - I can envision such a thing being useful as a way to sideload plugins.

Certain individual directories within /var/lib/grafana are already closed to world access. Something must set them that way.

👍 1

aknuds1 moved this from **To do** to **In progress** in **Backend Platform Squad** on Jul 15, 2020

aknuds1 commented on Jul 15, 2020 Contributor

Looking into how to solve this.

aknuds1 commented on Jul 15, 2020 Contributor

@marefr **@bergquist** Do you know where the permissions on /var/lib/grafana are dictated? Should we change its permissions to 750?

aknuds1 mentioned this issue on Jul 15, 2020

Database: Set 0640 permissions on SQLite database file #26339

Merged

aknuds1 commented on Jul 15, 2020 • edited Contributor

I've made a PR to change SQLite file permissions to 0600.

aknuds1 moved this from **In progress** to **Under review** in **Backend Platform Squad** on Jul 15, 2020

aknuds1 closed this as completed in #26339 on Jul 23, 2020

Backend Platform Squad automation moved this from **Under review** to **Done** on Jul 23, 2020

marefr added this to the **7.2** milestone on Aug 20, 2020

Assignees

aknuds1

Labels

area/backend/db area/security help wanted

Projects

No open projects

1 closed project

Milestone

7.2.0-beta1

Development

Successfully merging a pull request may close this issue.

Database: Set 0640 permissions on SQLite database file grafana/grafana

7 participants