

🎉 Welcome to Fedora Discussion! 🗨️

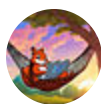
×

Check out the our [guide to navigation: tags, categories, and concepts](#), or add to our [tips and tricks](#).

Flatpak: “home” access allows trivial privilege escalation, what to do instead

🔗 Ask Fedora

#kde #wayland #flatpak #kde-plasma #bluetooth #howto #security-sig #flathub #permissions #dotfiles



boresquirrel

4 ✎ Apr 2024

[This Github issue describes the problem well](#) 26

If an app has the static filesystem permission for `home`, it can place this override file to give itself any possible permission.

```
mkdir ~/.local/share/flatpak/overrides
cat >> ~/.local/share/flatpak/overrides/my.awesome.App <<EOF
[Context]
shared=network;ipc
sockets=x11;wayland;fallback-x11;pulseaudio;session-bus;system-bus;ssh-auth;
pcsc;cups
devices=dri;kvm;shm;all
features=devel;multiarch;bluetooth;canbus
filesystems=host;host-os;host-etc;home
EOF
```

This concept is actually how [Flatseal](#) 18 works, placing override files for each app and thus modifying their permissions.

If this was only possible for reducing the permissions, it would be harmless and even useful. But it is a direct way for privilege escalation instead.

The issue was closed, which I find concerning. The general tone is

If an app has `home` permission, dont expect it to be secure.

I think this is pretty bad and there are 2 ways to tackle this.



This website uses cookies to function. The compliance people asked us to tell you.

[More information.](#)

Fine.

Apps that have **home** permission can no longer read and write

- your `~/.bashrc`
- your ssh and gpg keys
- these permission overrides
- ...

and much more. Flatpaks have no business in the dotfiles, [even though Cryptomator devs think it should](#) ¹⁶ .

And even if apps need that, they can specify the exact directories. This is how [Flatsweep](#) ¹⁵ does it, while Flatpak normally blocks access to `~/.var/app` (to allow “containerization”, while all apps with **home** permission could just change their permissions, lol)

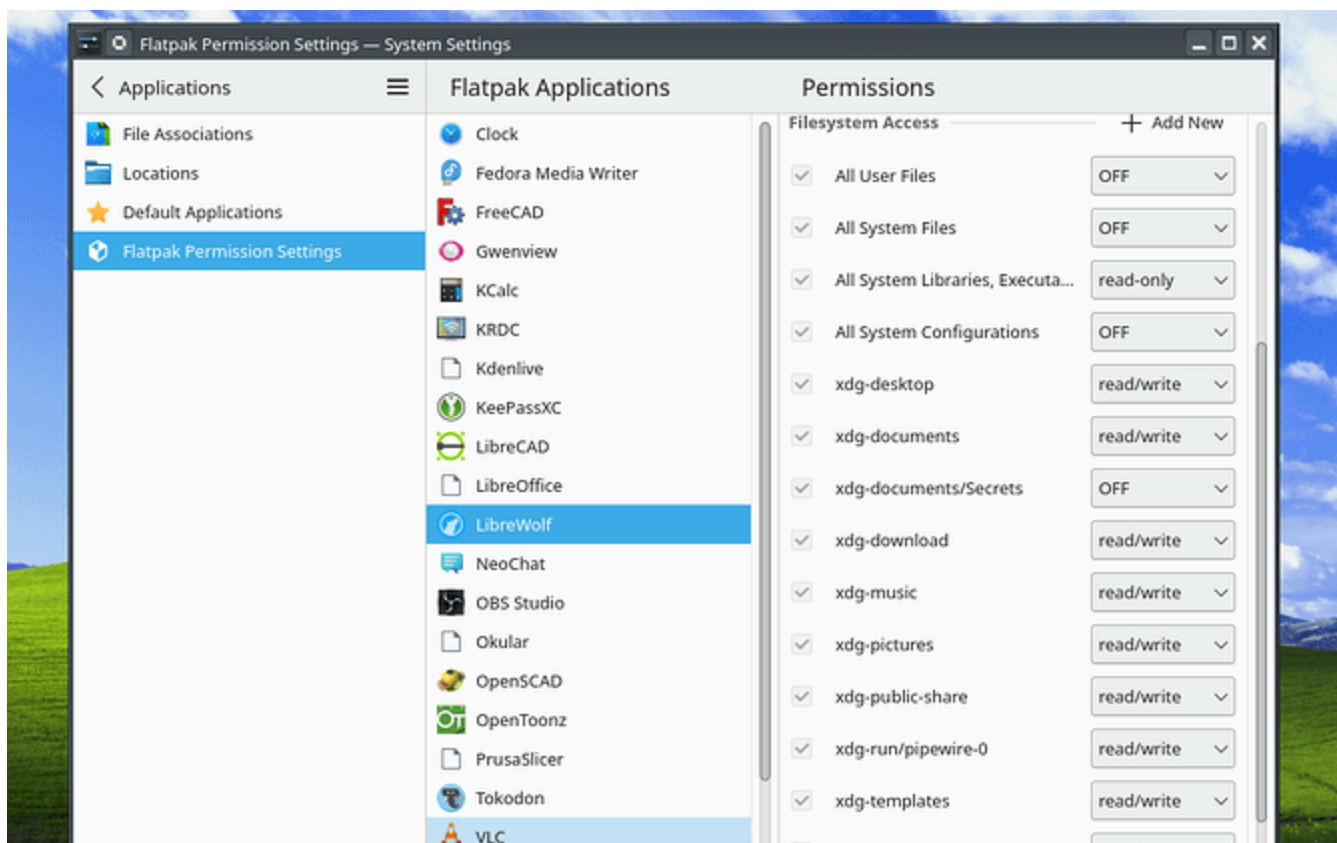
```
--filesystem=home/.var/app/",
--filesystem=/var/lib/flatpak/app:ro",
--filesystem=home/.local/share/flatpak/app:ro"
```

But this needs to be done at a Flatpak level, [see this issue](#) ⁵ .

2. Override for all apps with home permission

I really like [@pkmays' approach to this](#)

They used a general override for all apps, resulting in a permission page like this:



This works really well, but as a side effect (I think) breaks all preset permissions by apps. There are very few apps like Gnumeric that have too little permissions, but most have just the permissions they need.

So this would sometimes lead to extended privileges and lots of manual work (it is not a scaleable concept).

What would be a good way to do a function, all apps with `home` permission get such an override file placed? Best would be in a non user-writable directory.

Are there differences in `--user` and system installed apps?

 6



-  RPM and Flatpak security 1
-  Interesting topics of mine

2.3k

23

11






6

views

likes

links

users




3 months later


2.3k
views


23
likes


11
links


6
users











Reply

Related topics

Topic	Replies	Views	Activity
Workstation, Silverblue: preinstall Flatseal Project Discussion #silverblue-team #workstation-wg	8	840	Mar 2024
Add more xdg-directories by default? Ask Fedora #flatpak	3	464	May 2024
Flatpaks can't seem to access most folders, including /home Ask Fedora	4	6.6k	Mar 2024
Newbie questions Project Discussion #silverblue-team	6	612	Aug 2019
Flatpak office suites sensible filesystems permissions Project Discussion #silverblue-team	4	1.4k	Feb 2024

It's *your* OS.