Security Issue: Exposure of sensitive function, malicious user can arbitrary command via an execute_command d-bus method. #1796

Closed junorouse opened this issue on Sep 21, 2020 · 3 comments · Fixed by #2017

Labels Priority: High Type: Defect

junorouse commented on Sep 21, 2020 • edited

Describe the bug

We understand that the usability of `-e` option. (#720)
BTW, it must not be exposured in d-bus interfaces.

Expected behavior

guake must not exposure execute_command in d-bus interfaces.

Do not exposure execute_command in d-bus interface.

Actual behavior

guake exposure execute_command in d-bus interface.

To Reproduce

We can use gdbus to call an execute_command d-bus method.

```
$ gdbus call -e -d org.guake3.RemoteControl -o /org/guake3/RemoteControl -m org.guake3.RemoteControl.execute_command "id > /tmp/1234"
$ cat /tmp/1234
uid=1000(juno) gid=1000(juno)
groups=1000(juno),4(adm),20(dialout),21(fax),24(cdrom),25(floppy),26(tape),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),109(netdev),112(bluetooth),115(lpadmin),117(scan
```

```
juno@abcd:/tmp/p/$ guake --support
Usage: guake [options]

guake: error: no such option: --support
```

cc. @bbb1g

junorouse commented on Sep 21, 2020 • edited Author

And also execute_command_by_uuid is affected.

```
execute_command_by_uuid(in  s tab_uuid, in  s command);
```

Davidy22 added Priority: High Type: Defect labels on Sep 4, 2021

Davidy22 added a commit to Davidy22/guake that referenced this issue on Jan 20

`Fix arbitrary execution via dbus security flaw` ··· ✓ 709a242

Davidy22 added a commit to Davidy22/guake that referenced this issue on Jan 20

`Fix arbitrary execution via dbus security flaw` ··· ✓ e3d6711

Davidy22 mentioned this issue on Jan 20

Fix arbitrary execution via dbus security flaw #2017
Merged

gsemet closed this as completed in #2017 on Jan 27

gsemet pushed a commit that referenced this issue on Jan 27

`Fix arbitrary execution via dbus security flaw` ··· ✓ b769b3a

ghostshadow commented on Feb 16

Hi, it is nice, that you fix a potential security issue, but is there any concept for keeping the `-e` option working without the dbus call?
I use this option at a few places and would like to know now, if this option is going to be supported in the future or if i have to find another method for implementing my use cases.

Davidy22 commented on Feb 17 Collaborator

Only the dbus call has been disconnected, -e is still a flag

midnight-wonderer mentioned this issue on Feb 19

Security fix breaks `guake -e` #2042

Closed

Assignees

No one assigned

Labels

Priority: High Type: Defect

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

Fix arbitrary execution via dbus security flaw
Davidy22/guake

3 participants