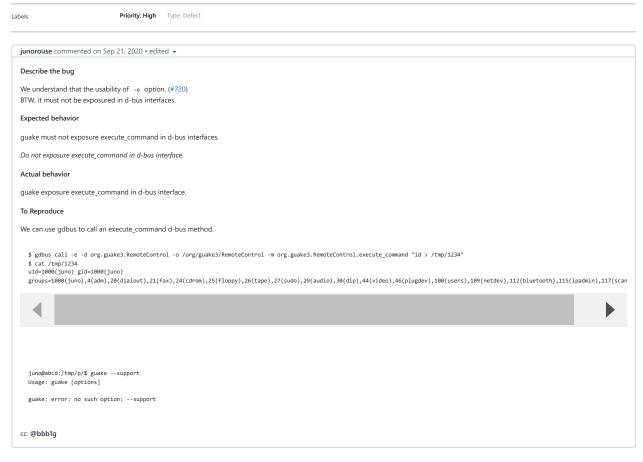
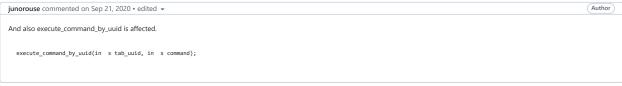


New issue

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







- 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 ...

 789a242

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

 Fix arbitrary execution via dbus security flaw ...

 483d6711

 Davidy22 mentioned this issue on Jan 20

 Fix arbitrary execution via dbus security flaw #2017

 Merged

 Sgemet closed this as completed in #2017 on Jan 27
- $\slash\hspace{-0.6em}$ $\slash\hspace{-0.6em}$ gsemet pushed a commit that referenced this issue on Jan 27
 - Fix arbitrary execution via dbus security flaw ...

Jump to bottom

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

 \square 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

