~~Bug 1196451~~ - ~~(CVE-2022-21946) VUL-0: CVE-2022-21946: cscreen: restrict usage of cscreen to a trusted set of users~~

Status: RESOLVED FIXED

Classification: Novell Products
Product: SUSE Security Incidents
Component: Audits
Version: unspecified
Hardware: Other Other

Priority: P5 - None **Severity**: Normal
Target Milestone: ---
Assigned To: Olaf Hering
QA Contact: Security Team bot

URL:
Whiteboard:
Keywords:

Depends on:
Blocks: ~~1196140~~
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2022-02-24 14:21 UTC by Matthias Gerstner
Modified: 2022-03-11 10:22 UTC (History)
CC List: 3 users (show)

See Also:
Found By: ---
Services Priority:
Business Priority:
Blocker: ---

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this bug.

Matthias Gerstner 2022-02-24 14:21:14 UTC Description

```
+++ This bug was initially created as a clone of ~~Bug #1196140~~

Currently cscreen ships this suoders rule:

```/etc/sudoers.d/cscreen
ALL ALL=(_cscreen) NOPASSWD:/usr/bin/screen
```

This means that *any* user in the system including accounts like 'nobody' can
attach to the shared screen session. This gives them also full access to the
capabilities of the _cscreen user, like a proper home directory in
```

/var/lib/cscreen where persistent data can be stored. Furthermore any shared information in existing cscreen sessions can be accessed, or arbitrary information can be placed into existing or newly created cscreen sessions.

Installation of the cscreen package alone is enough to enable most of this attack surface. Starting the daemon process is only necessary for the permanent cscreen background session to become available.

I recommend to adjust the cscreen package in a way that only members of a certain group are covered by the sudo rule. Ideally by introducing a separate group for this purpose (there already exists _cscreen, which could be used for this purpose).

Olaf Hering 2022-02-24 16:52:23 UTC Comment 1

I think the entire point of this is that everyone who can login to the console server must also be able to attach to the cscreen.

In case we want to go down the route of restricting access to users in the existing group _cscreen, how does the sudoers file need to look like?

Matthias Gerstner 2022-02-25 14:43:20 UTC Comment 2

(In reply to Olaf Hering from comment #1)

> I think the entire point of this is that everyone who can login to the
> console server must also be able to attach to the cscreen.

Yeah I get your use case, but between a security concern and a helpful feature there is hopefully some middle ground.

You could choose to grant access to all members of the users group or some such. However that would still be kind of implicit, and that the fact that the cscreen package is installed alone suddently grants additional privileges makes me feel uneasy on this.

> In case we want to go down the route of restricting access to users in the
> existing group _cscreen, how does the sudoers file need to look like?

A valid and hairy question given sudo's infamous syntax. This should do it:

```
%_cscreen ALL=(_cscreen) NOPASSWD:/usr/bin/screen
```

Olaf Hering 2022-02-25 16:16:54 UTC Comment 3

So lets do this change to the sudoers file.

Johannes Segitz 2022-03-09 12:12:55 UTC Comment 4

I pondered a bit if it makes sense to assign a CVE here. Matthias outlined some of the impact, additionally this grants access to the tty and dialout group to all users on the system. With all of that combined a CVE makes sense to me. Please use CVE-2022-21946 for this

Olaf Hering 2022-03-09 13:06:09 UTC Comment 5

Fixed upstream.
https://github.com/openSUSE/cscreen/commit/213b1f8424befeb453bd48eb29fd67f279fe4935

Olaf Hering 2022-03-09 13:09:32 UTC Comment 6

```
I'm not sure if "just installing cscreen.rpm" will do any harm.
But starting cscreen.service will indeed allow every user to attach to it.
```