~~Bug 1196446~~ - (CVE-2022-21945) VUL-0: CVE-2022-21945: cscreen: usage of fixed path /tmp/cscreen.debug

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 14:04 UTC by Matthias Gerstner
Modified:	2022-03-11 10:16 UTC (History)
CC List:	3 users (show)
See Also:	
Found By:	---
Services Priority:	
Business Priority:	
Blocker:	---

Attachments

bug1196446.patch (1.88 KB, text/plain) Details
2022-02-25 16:01 UTC, Olaf Hering

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

Note

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

Matthias Gerstner 2022-02-24 14:04:22 UTC Description

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

The cscreen package uses a fixed path /tmp/cscreen.debug in the script
/usr/bin/cscreen_update_config.sh:

```
function add_window()
{
    <...snip...>
```
```

```
    echo $_host >> /tmp/cscreen.debug
    echo $_status >> /tmp/cscreen.debug
    if [ -n "$_status" ];then
        echo "screen -x $session -X $_status" >> /tmp/cscreen.debug
        screen -x $session -X defhstatus "$_status" >>/tmp/cscreen.debug 2>&1
    fi
    echo "Add Window $TITLE: screen -x $session -X $COMMAND" >>/tmp/cscreen.debug
    <...snip...>
}
```

Luckily no one seems to be reading from there anymore.

Without symlink protection this could be a local DoS vector against the system.
By placing a FIFO in this location it could be a dedicated DoS and information
leak against the update script.

Please change the script either to drop this debug file by default, by using
an unpredictable temporary file name, or by using a safe location for the file
that is not accessible by every user in the system.

Olaf Hering 2022-02-25 12:19:51 UTC Comment 1

This script is called by orthos.
When do we intend to lift the embargo? I changed the location to /run/cscreen/

Matthias Gerstner 2022-02-25 14:47:25 UTC Comment 2

(In reply to Olaf Hering from comment #1)

> This script is called by orthos.
> When do we intend to lift the embargo? I changed the location to
> /run/cscreen/

It's up to us. I suggest when you have solutions ready for both issues then we can
publish it.

Olaf Hering 2022-02-25 16:01:31 UTC Comment 3

Created attachment 856583 [details]
~~bug1196446~~.patch

I think this change will fix the issue.

Matthias Gerstner 2022-02-28 12:39:31 UTC Comment 4

(In reply to ohering@suse.com from comment #3)

> Created attachment 856583 [details]
> ~~bug1196446~~.patch
>
> I think this change will fix the issue.

Yes, using the dedicated /run/ directory is good. I'm not quite sure about the
kind of debug output generated by these commands, could it be prudent to
protect the debug file from world and only allow e.g. members of the same
_cscreen group to read them?

Olaf Hering 2022-02-28 12:49:24 UTC Comment 5

yeah, I already planned to adjust the mask in tmpfile.conf.

Johannes Segitz 2022-03-09 10:16:22 UTC Comment 7

```
Please use CVE-2022-21945 for this. For the other issue I'm still a bit torn and
need to think about it more
```

Olaf Hering 2022-03-09 10:26:47 UTC Comment 8

```
Fixed upstream.
https://github.com/openSUSE/cscreen/commit/e9a698cc317125300ff49d99b841f537a61fe65f
```