

Bug 1193484 (CVE-2021-36781) VUL-0: CVE-2021-36781: parsec: dangerous 777 permissions for /run/parsec

Status: RESOLVED FIXED

Classification: openSUSE

Product: openSUSE Tumbleweed

Component: Security

Version: Current

Hardware: Other Other

Priority: P5 - NoneSeverity: Normal (vote)

Target Milestone: ---

Assigned To: Guillaume GARDET

QA Contact: E-mail List

URL:

Whiteboard:

Keywords:

Depends on:

Blocks:

Create test case

Clone This Bug

Reported: 2021-12-07 13:27 UTC by Matthias Gerstner

Modified: 2021-12-09 14:30 UTC (History)

CC List: 2 users (show)

See Also:

Found By: ---

Services Priority:

Business Priority:

Blocker: ---

Show dependency tree / graph

Attachments

- simple reproducer (428 bytes, text/x-script.python)

Details
- 2021-12-09 13:15 UTC, Matthias Gerstner
- 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 Gerstner2021-12-07 13:27:46 UTC

Description

The parsec package installs a systemd-tmpfiles configuration that is checked in into openSUSE:Factory/parsec/parsec.conf. This configuration contains the following line since the most recent submission:

```
...
d    /run/parsec    777    parsec parsec-clients    -    -
...
```

This means that /run/parsec is world-readable and just any local user can change its contents. From looking at the parsec source code it looks like the service is creating a UNIX domain socket for clients to connect in there.

This in turn means that a local attacker can replace this UNIX domain socket and have clients talking to an imposter service. Furthermore it also poses a denial-of-service vector.

Please fix these directory permissions, they should be 755 at most.

This seems to be a SUSE specific bug or did you package such permissions also for other distributions? If it is SUSE specific then we can assign one of our own SUSE CVEs for this issue.

Guillaume GARDET2021-12-09 10:37:45 UTC

Comment 1

This is a permission on the folder, not on the files inside.

And parsec checks the ID of the current user, so I do not think this is a problem.

Guillaume GARDET2021-12-09 11:05:25 UTC

Comment 2

After checking with parsec maintainers, they recommend to use 755 (or 750 if users need to be part of parsec-clients).

So, I will fix it right now.

Guillaume GARDET2021-12-09 11:07:29 UTC

Comment 3

Fixed in <https://build.opensuse.org/request/show/937755>

And only openSUSE/SUSE is affected.

Guillaume GARDET2021-12-09 11:10:52 UTC

Comment 4

FTR, parsec doc recommends 755: https://parallaxsecond.github.io/parsec-book/parsec_service/install_parsec_linux.html

Matthias Gerstner2021-12-09 13:15:29 UTC

Comment 5

Created [attachment 854434 \[details\]](#)

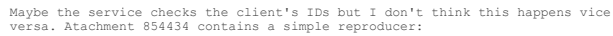
simple reproducer

Matthias Gerstner2021-12-09 13:22:01 UTC

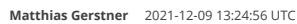
Comment 6

```
(In reply to guillaume.gardet@arm.com from comment #1)
> This is a permission on the folder, not on the files inside.
```

> And parsec checks the ID of the current user, so I do not think this is a problem



This shows that a compromised "nobody" user can replace the parsec UNIX domain socket and can react to client requests. In this case the incoming requests are simply echoed resulting in an error and a kind of denial of service. Maybe the effects could be worse.



Comment 7

Comment 8

Comment 9

This is an autogenerated message for OBS integration:
This bug (1193484) was mentioned in
<https://build.opensuse.org/request/show/937794> Factory / parsec
<https://build.opensuse.org/request/show/937795> Backports:SLE-15-SP4 / parsec