~~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 - None **Severity**: Normal (vote)
Target Milestone:	---
Assigned To:	Guillaume GARDET
QA Contact:	E-mail List
URL:	
Whiteboard:	
Keywords:	
Depends on:	
Blocks:	

Show dependency tree / graph

- 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:	---

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 Gerstner 2021-12-07 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 GARDET 2021-12-09 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 GARDET 2021-12-09 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 GARDET 2021-12-09 11:07:29 UTC Comment 3

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

And only openSUSE/SUSE is affected.

Guillaume GARDET 2021-12-09 11:10:52 UTC Comment 4

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

Matthias Gerstner 2021-12-09 13:15:29 UTC Comment 5

Created attachment 854434 [details]
simple reproducer

Matthias Gerstner 2021-12-09 13:22:01 UTC Comment 6

First of all: Thanks for fixing the issue.

(In reply to guillaume.gardet@arm.com from comment #1)

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

yes, but world-writable permissions mean that all the files inside can be replaced by anybody.

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

Maybe the service checks the client's IDs but I don't think this happens vice versa. Atachment 854434 contains a simple reproducer:

```
root# systemctl start parsec.service
root# sudo -u nobody python3 replace_parsec.py
<socket.socket fd=4, family=AddressFamily.AF_UNIX, type=SocketKind.SOCK_STREAM,
proto=0, laddr=/run/parsec/parsec.sock>
Connection from Received
b'\x10\xa7\xc0^\x1e\x00\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x

root# parsec-tool list-providers
[ERROR] Error spinning up the BasicClient: client is missing an implicit provider
```

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.

Matthias Gerstner 2021-12-09 13:24:56 UTC Comment 7

Publishing.

Johannes Segitz 2021-12-09 13:51:59 UTC Comment 8

Please use CVE-2021-36781 for this

OBSbugzilla Bot 2021-12-09 14:30:09 UTC 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