Bug 1171649 - (CVE-2020-8021) VUL-0: CVE-2020-8021: OBS: unauthorized read access to files where sourceaccess is disabled via a crafted _service file

Status: NEW

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

Priority: P3 - Medium **Severity**: Normal
Target Milestone: ---
Assigned To: Adrian Schröter
QA Contact: Security Team bot

URL: https://smash.suse.de/issue/259581/
Whiteboard:
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-05-14 08:17 UTC by Alexandros Toptsoglou
Modified: 2020-10-01 12:12 UTC (History)
CC List: 6 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.

Alexandros Toptsoglou 2020-05-14 08:17:24 UTC — Description

```
through an email

Hi,

currently, it is possible for an unprivileged user to access (read-only)
the files of an OBS package where the sourceaccess/access is disabled in the
meta. The exploit is documented in the attached mergeservice_exploit.txt
file. I also attached a potential patch (see the
0001-backend-bs_srcserver-Forbid-the-creation-of-a-_link-.patch file).

md5sum                                  attached file
7d6787b7d854381da5d672fb29163c14  mergeservice_exploit.txt
9b7d3878d70acef3bf7f2cbfb0565bbc  0001-backend-bs_srcserver-Forbid-the-creation-of-
a-_link-.patch
```

Adrian Schröter 2020-05-14 08:19:46 UTC — Comment 3

```
The reporter was actually

Marcus Hüwe <suse-tux@gmx.de>
```

Matthias Gerstner 2020-05-14 09:49:47 UTC — Comment 4

```
I don't think this is actually news. In the OBS server side review I found
different ways to get around this restriction. See bug 1085033 comment 27
section "sourceaccess disabled".
```

Marcus Hüwe 2020-05-14 22:15:58 UTC — Comment 5

```
(In reply to Matthias Gerstner from comment #4)

> I don't think this is actually news. In the OBS server side review I found
> different ways to get around this restriction. See bug 1085033 comment 27
> section "sourceaccess disabled".


Ah ok - I'm not authorized to access that bug...
Without knowing the details, a most likely "naive" question: if the issue is
known, why don't we fix it?
```

Adrian Schröter 2020-05-15 05:49:06 UTC — Comment 6

```
we will fix it and I see actually not a reference to mergeservice in the mentioned
bug rereport.
```

Marcus Meissner 2020-05-15 15:48:53 UTC — Comment 7

```
JUst to be clear, this issue had no CVE yet? And is confirmed to be a valid
security isssue?

Then we would assign a CVE.
```

Adrian Schröter 2020-05-15 18:03:12 UTC — Comment 8

Yes, it is valid and has no CVE yet.

Marcus Meissner 2020-05-15 18:33:53 UTC Comment 9

Please use CVE-2020-8021.

Johannes Segitz 2020-05-19 12:51:40 UTC Comment 11

Making public to allow for publishing of CVE

Utkarsh Gupta 2020-10-01 11:19:59 UTC Comment 12

Hello,

Any ETA on this? Is there a fix out?
If so, could you point me to the fixing commit? :)

Thanks!

Marcus Hüwe 2020-10-01 12:12:00 UTC Comment 13

(In reply to Utkarsh Gupta from comment #12)

> Any ETA on this? Is there a fix out?
> If so, could you point me to the fixing commit? :)
>

It is fixed in commit 7323c904f86ba9e04065c23422d06c03647589fb ("bs_srcserver: Forbid the creation of a _link in mergeservicerun") (see [1]).

[1] https://github.com/openSUSE/open-build-service/commit/7323c904f86ba9e04065c23422d06c03647589fb

---