~~Bug 1164131 - (CVE-2020-8014) VUL-0: CVE-2020-8014: kopano-python-services: Local privilege escalation from kopano to root in kopano-spamd subpackage~~

Status: RESOLVED FIXED

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

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

URL:
Whiteboard:
Keywords:

Depends on:
Blocks: 1154062
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2020-02-18 14:53 UTC by Johannes Segitz
Modified: 2020-06-24 13:21 UTC (History)
CC List: 2 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.

Johannes Segitz 2020-02-18 14:53:52 UTC — Description

```
300 %post -n kopano-spamd
301 chown -Rh kopano:kopano /var/log/kopano 2>/dev/null || :
302 chown kopano:kopano /var/lib/kopano/spamd 2>/dev/null || :

chown runs as root, /var/lib/kopano is controlled by user kopano. By watching for
the change in /var/log/kopano I can easily time when to change
/var/lib/kopano/spamd to a symlink.

POC:
sh-5.0$ id
uid=464(kopano) gid=463(kopano) groups=463(kopano)
sh-5.0$ ls -l /test/shadow
-rwxr-x--- 1 root root 1249 Feb 18 14:31 /test/shadow
sh-5.0$ ./poc_kopano /var/log/kopano/ /var/lib/kopano/
[+] watching /var/log/kopano/
[+] added link
total 12K
drwxr-xr-x  2 root   root   4.0K Feb 18 14:31 .
drwxr-xr-x 23 root   root   4.0K Feb 18 14:31 ..
-rwxr-x---  1 kopano kopano 1.3K Feb 18 14:31 shadow

Once poc_kopano runs force reinstallation of kopano-spamd as root:
zypper in -f kopano-spamd

poc_kopano uses inotify to watch /var/log/kopano and symlinks /test/shadow to
/var/lib/kopano/spamd once it see's the first chown
```

Johannes Segitz 2020-02-18 14:55:12 UTC — Comment 1

```
This issue will be handled according to our disclosure policy outlined in
https://en.opensuse.org/openSUSE:Security_disclosure_policy

The information listed here is not public. Please
- do not talk to other people about this unless they're involved in fixing the
issue
- do not make this bug public

In accordance with our policy we will make this issue public latest at
Internal CRD: 2020-05-18
This is the latest possible date and we prefer to make it public earlier if the
situation allows it. In that case we'll post a comment here setting the new
date.

Only a member of the security team is allowed to make this issue public. Please
speak to us if you want to take part in  the public disclosure.

In doubt please talk to us on IRC (#security) or send us a mail (security@suse.de).
```

Jan Engelhardt 2020-02-18 15:27:35 UTC — Comment 2

```
What is the actual bug? Is it the scriptlet chown/chmod? Is there other issues
outside the specfile?
```

Johannes Segitz 2020-02-18 16:09:45 UTC — Comment 3

```
(In reply to Jan Engelhardt from comment #2)
The usage of chown in the user controlled path is the issue
302 chown kopano:kopano /var/lib/kopano/spamd 2>/dev/null || :
```

For the recursive chown there's another bug, but that will not receive a CVE since it's not exploitable on default systems

---

Johannes Segitz 2020-02-25 07:37:31 UTC Comment 5

(In reply to Jan Engelhardt from comment #2)
Sorry for the confusion. I made comment 0 public. I assumed you as assignee can see it even if it's private, but apparently not

---

Johannes Segitz 2020-05-13 08:17:47 UTC Comment 6

Please note that this will be made public soon, please submit. Thank you

---

Jan Engelhardt 2020-06-09 19:06:05 UTC Comment 7

waiting in openSUSE:Maintanenace:12676

Jan Engelhardt 2020-06-24 12:06:39 UTC Comment 8

Is there anything else I need to do here to get this moving?

Marcus Meissner 2020-06-24 12:16:23 UTC Comment 9

openqa was stuck:

https://openqa.opensuse.org/tests/1281592#step/qam_zypper_patch/12

0| 2020-05-28 12:38:41 <1> linux-fyje(4409) [zypp::solver] SATResolver.cc(problems):1183 libkcarchivercore0-8.6.0.0-lp151.2.5.x86_64 requires libmapi.so.1(KC_8.6)(64bit), but this requirement cannot be provided

I think its ok to release, i will override openqa.

Marcus Meissner 2020-06-24 13:21:02 UTC Comment 10

reelased
