Bug 1180669 - (CVE-2020-8032) VUL-0: CVE-2020-8032: cyrus-sasl: Local privilege escalation to root due to insecure tmp file usage

Status: IN_PROGRESS

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

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

URL:
Whiteboard: CVSSv3.1:SUSE:CVE-2020-8032:8.4:(AV:L...
Keywords:

Depends on:
Blocks:
Show dependency tree / graph

- Create test case
- Clone This Bug

Reported: 2021-01-07 15:51 UTC by Johannes Segitz
Modified: 2021-04-20 09:14 UTC (History)
CC List: 3 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 2021-01-07 15:51:29 UTC Description

```
In cyrus-sasl.spec
217 %pre
218 #Convert password file from berkely into gdbm
219 #In %pre the existing file will be dumped out
220 if [ -e /etc/sasldb2 ]; then
221 cat <<EOF > /tmp/saslpw.awk
222 {
223         split(\$0,b,/\\\00/)
224         if( b[3] == "userPassword" ) {
225                 user=b[1]
226                 domain=b[2]
227         } else {
228                 if( user != "" ) {
229                         printf("echo '%s' | saslpasswd2 -p -u %s
%s\n",substr(b[1],2),user,domain)
230                         user = ""
231                         domain = ""
232                 }
233         }
234 }
235 EOF
236 db_dump -p /etc/sasldb2 | gawk -f /tmp/saslpw.awk > /var/adm/update-
scripts/saslpwd

allows users on the system to escalate to root. If a user creates /tmp/saslpw.awk
before this runs and then monitors the file (e.g. inotifywait /tmp/saslpw.awk) he
can change it to arbitrary content after cat writes it, but before gawk is called.
When something like this
BEGIN {system("chown johannes /etc/shadow")}
is written to the file this allows escalating to root as this snippet is executed
with root privileges.

Rating low since this can only be triggered once and the race is hard to win.
Reproduction:
as root (if /etc/sasldb2 doesn't exist)
cp /etc/postfix/relocated.db /etc/sasldb2
otherwise db_dump will fails and it stops there.

As user:
inotifywait /tmp/saslpw.awk; echo 'BEGIN {system("chown johannes /etc/shadow")}' >
/tmp/saslpw.awk

Then as root install the package
zypper in -y -f cyrus-sasl

It's hard to win the race, but with a more optimized exploit this should work.

This was recently introduced into Factory, so we need a CVE for it: CVE-2020-8032

Please use a safe way to create temporary files or (better) don't write them to a
location that users can influence.

CRD: 2021-04-07
as specified in https://en.opensuse.org/openSUSE:Security_disclosure_policy, but I
would ask you to fix it right away to keep the window where this can be abused
short.
```

Johannes Segitz 2021-02-11 14:52:40 UTC Comment 4

```
can you please submit for Factory? Then we can make it public and publish the CVE
```

Peter Varkoly 2021-02-12 13:03:25 UTC Comment 5

(In reply to Johannes Segitz from comment #4)

> can you please submit for Factory? Then we can make it public and publish
> the CVE

https://build.opensuse.org/request/show/871430

OBSbugzilla Bot 2021-02-18 13:00:06 UTC Comment 6

This is an autogenerated message for OBS integration:
This bug (1180669) was mentioned in
https://build.opensuse.org/request/show/873374 Factory / cyrus-sasl

---

OBSbugzilla Bot 2021-02-19 09:10:09 UTC Comment 7

This is an autogenerated message for OBS integration:
This bug (1180669) was mentioned in
https://build.opensuse.org/request/show/873673 Factory / cyrus-sasl

---

Johannes Segitz 2021-02-25 08:36:23 UTC Comment 8

thanks

Johannes Segitz 2021-02-25 09:05:45 UTC Comment 9

submit to Factory was declined, please have a look

OBSbugzilla Bot 2021-02-25 15:30:06 UTC Comment 10

This is an autogenerated message for OBS integration:
This bug (1180669) was mentioned in
https://build.opensuse.org/request/show/875151 Factory / cyrus-sasl

---

OBSbugzilla Bot 2021-02-25 18:40:06 UTC Comment 11

This is an autogenerated message for OBS integration:
This bug (1180669) was mentioned in
https://build.opensuse.org/request/show/875214 Factory / cyrus-sasl

---

OBSbugzilla Bot 2021-02-27 13:20:06 UTC Comment 12

This is an autogenerated message for OBS integration:
This bug (1180669) was mentioned in
https://build.opensuse.org/request/show/875610 Factory / cyrus-sasl

---

Peter Varkoly 2021-03-10 18:51:29 UTC Comment 13

Fix is accepted
