Privilege escalation to root with core file dump

Bug #1912326 reported by Itai Greenhut on 2021-01-19

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	Brian Murray	
Xenial	Fix Released	Undecided	Marc Deslauriers	
Bionic	Fix Released	Undecided	Marc Deslauriers	
Focal	Fix Released	Undecided	Marc Deslauriers	
Groovy	Fix Released	Undecided	Marc Deslauriers	
Hirsute	Fix Released	Undecided	Brian Murray	

Bug Description

Vulnerabilities in Apport in ubuntu 20.04/18.04

==

Author information

Itai Greenhut(@Gr33nh4t)

Aleph Research by HCL Appscan

<email address hidden>

SUMMARY

We found several vulnerabilities in apport program which work on default installations of ubuntu 20.04/18.04.

We were able to chain those vulnerabilities together to get local privilege escalation to root from an unprivileged user.

Issue 1: Bypass drop_privileges and set Uid and Gid to arbitrary value

----

real_uid and real_gid are set by reading /proc/pid/status file and parsing its content.

"get_pid_info" function will iterate through each line and if a line starts with "Uid:" or "Gid:" it takes the first argument in that line and puts it into real_uid and real_gid variables.

We were able to bypass this by crashing a process with a file name set to "a\rUid: 0\rGid: 0".

When the process crashed, we "injected" those values to /proc/pid/status file (in the Name field), causing apport to never really drop privileges in the function drop_privileges(real_uid now is 0 and real_gid is also 0).

By having full control over real_uid and real_gid we were able to bypass the suid check on "write_user_coredump" function.

Issue 2: Bypass get_process_startime check

Apport checks if the process was replaced after the crash by comparing between apport_start and process_start.

process_start gets the start time of the process by parsing the content of /proc/pid/stat file.

The start time is extracted from the 22 column of the /proc/pid/stat file.

We were able to bypass this check by recycle the pid with a process with " "(space) in its filename, causing get_process_starttime to return the wrong value (which is smaller than apport_start).

Issue 3: delay apport get_pid_info by 30 seconds and recycle pid to suid process

----

We were able to delay apport get_pid by 30 seconds from the process creation by acquiring the lock file of apport.

We were able to lock the file by creating a fifo file with a predictable name file crash in /var/log, and then create a new instance of apport.

Now when we create another apport instance it will then be locked for 30 seconds before getting a timeout.

We can release the lock file of the first instance by writing to the fifo file.

Exploitation:

Our main goal in the exploitation is to write core file owned by root with our content to an arbitrary directory.

Apport creates a core file in the current directory of the crashed process.

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 Murray
- Itai Greenhut

May be notified

- Alejandro J. Alva...
- Ashani Holland
- Benjamin Drung
- Bjoern
- Bruno Garcia
- CRC
- Calub Viem
- Cemirtan Igor Gri...
- Charlie_Smotherman
- Christina A Reitb...
- David
- Debian PTS
- Dmitriev Artem An...
- Doraann2
- Felix K.
- Franko Fang
- Hans Christian Holm
- HaySayCheese
- Hidagawa
- Jader Gabriel
- Jesse Jones
- José Alfonso
- Kees Cook
- Kshitij Mehrotra
- Marc Deslauriers
- Masoud shokohi
- Matt j
- Matvej Jurbin
- Micah Gersten
- Michael Rowland H...
- Mr. MInhaj
- Name Changed
- Nick
- PCTeacher012
- Paolo Topa
- PechayClub Inc.
- Peter Bullert
- Philip Muškovac
- Punnsa
- Richard Barnes
- Richard Seguin
- Richard Williams
- Rob Linc
- Rudra Saraswat
- Ryan Garrett
- Tom Weiss
- Ubuntu Foundation...
- Ubuntu Lumina
- Ubuntu Security Team
- Ubuntu Touch seed...
- Vasanth
- Vic Parker
- Warren White
- ahepas
- ali
- basilisgabri
- cornelis stravers
- dsfkj dfjx
- dvergspett
- eoininmoran
- ganesh
- linuxgijs
- majid hussain
- miked

As seen before on other apport exploits, we will create a core file in /etc/logrotate.d/ directory and execute a root shell.

In order to exploit those issues to gain local privilege escalation we need to perform the following steps:

1. Create unpackaged=true configuration in ~/.conf/apport/settings

2. mkfifo a predictable file of a decoy process.

3. Run the decoy process causing the first apport instance to "hang".

4. Create a symlink to /usr/bin/sudo with the name "a\rUid: 0\rGid: 0"

5. chdir to desired directory.

6. Create the crash program.

7. Fork lots of new processes to make the pid wrap to crash_program_pid - 1.

8. Send SIGSEGV to crash the program and trigger an additional apport instance.

9. Send SIGKILL to terminate the program and release crash_program_pid.

10. Create new process with fork and execve("a/rUid: 0\rGid: 0"). (The crafted file name)

11. Release the first process by writing to the fifo file.

The second apport instance will continue with execution and create a core dump in the current directory of the new suid process.

Now we have a root owned core file in desired directory, we can exploit this by having a valid configuration for logrotate inside the core dump and place the core dump inside /etc/logrotate.d/ directory.

CREDITS

Please credit "Itai Greenhut(@Gr33nh4t) from Aleph Research by HCL Appscan" for those issues.

Please note that we follow the community standard of 90 days before public disclosure please coordinate your patch release date with us.

Attaching poc of the exploit, run as follows:
1. tar zxvfm exploit.tar.gz
2. cd exploit
3. ./exploit.sh

Best regards,
Itai Greenhut
Aleph Research by HCL Appscan

Related branches

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

CVE References

2021-25682

2021-25683

2021-25684

Itai Greenhut (itaig) wrote on 2021-01-19: #2

To gain the root shell with the exploit demo run on another window:
1. nc -l -p 1234
2. change the time to 23:59:50

Marc Deslauriers (mdeslaur) wrote on 2021-01-20: #3

Thanks for reporting this issue. We are investigating it, and will assign CVEs.

Seth Arnold (seth-arnold) wrote on 2021-01-21: #4

Hello, we've assigned three CVEs for these findings:

CVE-2021-25682 error parsing /proc/pid/status
CVE-2021-25683 error parsing /proc/pid/stat
CVE-2021-25684 stuck reading fifo

Thanks

Marc Deslauriers (mdeslaur) on 2021-01-22

Changed in apport (Ubuntu Xenial):
assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in apport (Ubuntu Bionic):
assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in apport (Ubuntu Focal):
assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in apport (Ubuntu Groovy):
assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in apport (Ubuntu Hirsute):
assignee:nobody → Marc Deslauriers (mdeslaur)
Changed in apport (Ubuntu Xenial):
status:New → In Progress
Changed in apport (Ubuntu Bionic):
status:New → In Progress
Changed in apport (Ubuntu Focal):
status:New → In Progress
Changed in apport (Ubuntu Groovy):
status:New → In Progress

mmmen
nikonikic42
projevie@hotmail.com
qadir
sankaran
ubuntu18
van
नेपाली भाषा समायो...

Patches

apport.patch

Add patch

Changed in apport (Ubuntu Hirsute):
status:New → In Progress

Marc Deslauriers (mdeslaur) wrote on 2021-01-26: #5

apport.patch (9.9 KiB, text/plain)

Hi,

Attached is the patch we plan on using.

We propose making this public and releasing updates on 2020-02-02 18:00:00 UTC.
Is that date acceptable for you?

Thanks!

Marc Deslauriers (mdeslaur) wrote on 2021-01-26: #6

err, of course I meant 2021-02-02 18:00:00 UTC.

Itai Greenhut (itaig) wrote on 2021-01-27: #7

Hi,
Thank you for the fast response!
Yes 2021-02-02 18:00:00 UTC would be great date to post fixes.

As we plan to post in our blog with POC attached as well, we will wait additional week until 2021-02-09 with our blog post(as requested in your disclosure policy). Would it be OK?

The patch looks great! but I noticed that os.open would still be blocked on FIFO files, maybe O_NONBLOCK would help?

Thank you,
Itai Greenhut

Marc Deslauriers (mdeslaur) wrote on 2021-01-27: #8

> As we plan to post in our blog with POC attached as well, we will wait additional week until 2021-02-09 with our blog post(as requested in your disclosure policy). Would it be OK?

Yes, that would be perfect. Thanks!

> The patch looks great! but I noticed that os.open would still be blocked on FIFO files, maybe O_NONBLOCK would help?

Oh, thanks! I definitely forgot to put O_NONBLOCK there. Nice catch!

Marc.

Itai Greenhut (itaig) wrote on 2021-01-31: #9

Thank you!

I have deleted the attachment so the exploit code won't become public on the same day as the fix.

Itai

Launchpad Janitor (janitor) wrote on 2021-02-02: #10

This bug was fixed in the package apport - 2.20.11-0ubuntu50.5

```
---------------
apport (2.20.11-0ubuntu50.5) groovy-security; urgency=medium

  * SECURITY UPDATE: multiple security issues (LP: #1912326)
    - CVE-2021-25682: error parsing /proc/pid/status
    - CVE-2021-25683: error parsing /proc/pid/stat
    - CVE-2021-25684: stuck reading fifo
    - data/apport: make sure existing report is a regular file.
    - apport/fileutils.py: move some logic here to skip over manipulated
      process names and filenames.
    - test/test_fileutils.py: added some parsing tests.

 -- Marc Deslauriers <email address hidden> Tue, 26 Jan 2021 07:21:46
-0500
```

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

Launchpad Janitor (janitor) wrote on 2021-02-02: #11

This bug was fixed in the package apport - 2.20.9-0ubuntu7.23

```
---------------
apport (2.20.9-0ubuntu7.23) bionic-security; urgency=medium

  * SECURITY UPDATE: multiple security issues (LP: #1912326)
    - CVE-2021-25682: error parsing /proc/pid/status
    - CVE-2021-25683: error parsing /proc/pid/stat
    - CVE-2021-25684: stuck reading fifo
    - data/apport: make sure existing report is a regular file.
    - apport/fileutils.py: move some logic here to skip over manipulated
      process names and filenames.
    - test/test_fileutils.py: added some parsing tests.

 -- Marc Deslauriers <email address hidden> Tue, 26 Jan 2021 07:21:46
-0500
```

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

Launchpad Janitor (janitor) wrote on 2021-02-02: #12

This bug was fixed in the package apport - 2.20.1-0ubuntu2.30

```
---------------
apport (2.20.1-0ubuntu2.30) xenial-security; urgency=medium

  * SECURITY UPDATE: multiple security issues (LP: #1912326)
    - CVE-2021-25682: error parsing /proc/pid/status
    - CVE-2021-25683: error parsing /proc/pid/stat
    - CVE-2021-25684: stuck reading fifo
    - data/apport: make sure existing report is a regular file.
    - apport/fileutils.py: move some logic here to skip over manipulated
      process names and filenames.
    - test/test_fileutils.py: added some parsing tests.

 -- Marc Deslauriers <email address hidden> Tue, 26 Jan 2021 07:21:46
-0500
```

Changed in apport (Ubuntu Xenial):
status: In Progress → Fix Released

Launchpad Janitor (janitor) wrote on 2021-02-02: #13

```
This bug was fixed in the package apport - 2.20.11-0ubuntu27.16

---------------
apport (2.20.11-0ubuntu27.16) focal-security; urgency=medium

  * SECURITY UPDATE: multiple security issues (LP: #1912326)
    - CVE-2021-25682: error parsing /proc/pid/status
    - CVE-2021-25683: error parsing /proc/pid/stat
    - CVE-2021-25684: stuck reading fifo
    - data/apport: make sure existing report is a regular file.
    - apport/fileutils.py: move some logic here to skip over manipulated
      process names and filenames.
    - test/test_fileutils.py: added some parsing tests.

 -- Marc Deslauriers <email address hidden> Tue, 26 Jan 2021 07:21:46
-0500
```

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

Brian Murray (brian-murray) on 2021-02-03

Changed in apport (Ubuntu Hirsute):
assignee: Marc Deslauriers (mdeslaur) → Brian Murray (brian-murray)

Launchpad Janitor (janitor) wrote on 2021-02-03: #14

```
This bug was fixed in the package apport - 2.20.11-0ubuntu57

---------------
apport (2.20.11-0ubuntu57) hirsute; urgency=medium

  * SECURITY UPDATE: multiple security issues (LP: #1912326)
    - CVE-2021-25682: error parsing /proc/pid/status
    - CVE-2021-25683: error parsing /proc/pid/stat
    - CVE-2021-25684: stuck reading fifo
    - data/apport: make sure existing report is a regular file.
    - apport/fileutils.py: move some logic here to skip over manipulated
      process names and filenames.
    - test/test_fileutils.py: added some parsing tests.

 -- Brian Murray <email address hidden> Tue, 02 Feb 2021 12:42:44 -0800
```

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

Marc Deslauriers (mdeslaur) on 2021-02-04

information type: Private Security → Public Security

Benjamin Drung (bdrung) on 2022-06-27

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

See full activity log

To post a comment you must log in.