# Unhandled exception in check_ignored()

Bug #1877023 reported by Seong-Joong Kim on 2020-05-06

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 | Medium | Unassigned | |

## Bug Description

```
Hi,

I have found a security issue on apport 2.20.11 and earlier.

## Vulnerability
apport 2.20.11 and earlier have an unhandled exception vulnerability
during parsing apport-ignore.xml.
An attacker can cause a denial of service (i.e., application crash) via a
crafted apport-ignore.xml file.

## Description
Reports can be suppressed by blacklisting in apport-ignore.xml.

This is an example of apport-ignore.xml

<?xml version="1.0" ?>
<apport>
  <ignore mtime="1461374304" program="/opt/sublime_text/sublime_text"/>
  <ignore mtime="1453471676" program="/bin/sleep"/>
  <ignore mtime="1452699271" program="/usr/bin/strace"/>
</apport>

Unfortunately, it may cause an unhandled exception when 'mtime' attribute
is specified as a string value, not a number like this.

<?xml version="1.0" ?>
<apport>
  <ignore mtime="string" program="/bin/sleep"/>
</apport>

It may disrupt apport service and allow an attacker to potentially enable
a denial of service via local access.

The flaw lies in improper exception handling of 'mtime' attribute in
apport-ignore.xml (see https://git.launchpad.net/ubuntu/+source/apport/
tree/apport/report.py?h=applied/ubuntu/devel#n1104).

## Log
Here is /var/log/apport.log when the above exception occurs.

ERROR: apport (pid 25904) Tue May 5 18:38:21 2020: Unhandled exception:
Traceback (most recent call last):
  File "/usr/share/apport/apport", line 629, in <module>
    if info.check_ignored():
  File "/usr/lib/python3/dist-packages/apport/report.py", line 1082, in
check_ignored
    if float(ignore.getAttribute('mtime')) >= cur_mtime:
ValueError: could not convert string to float: 'string'

Sincerely,
```

See original description

Tags: patch

## Related branches

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

## CVE References

2020-11936

2020-15701

2020-15702

Seong-Joong Kim (sungjungk) on 2020-05-11

**description:** updated

Seong-Joong Kim (sungjungk) wrote on 2020-05-12: #1

unhandled-XML-exception.patch (811 bytes, text/plain)

```
Uncaught exception on malformed XML declaration.
Invalid data in the XML declaration causes an exception of a type that was
not handled properly in the parser and leads an unexpected exception.
Please check the attached patch.
```

Seong-Joong Kim (sungjungk) on 2020-05-13

**information type:** Private Security → Public Security

Seong-Joong Kim (sungjungk) on 2020-05-18

**affects:** apport → apport (Ubuntu)

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

Seong-Joong Kim
Ubuntu Review Team

May be notified

Alejandro J. Alva...
Ashani Holland
Benjamin Drung
Brian Murray
Bruno Garcia
CRC
Charlie_Smotherman
Christina A Reitb...
Debian PTS
Doraann2
Franko Fang
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 Muškovac
Punnsa
Richard Seguin
Richard Williams
Tom Weiss
Ubuntu Foundation...
Ubuntu Security Team
Ubuntu Touch seed...
Vasanth
Vic Parker
ahepas
basilisgabri
dsfkj dfjx
eoininmoran
ganesh
linuxgijs
miked
nikonikic42
projevie@hotmail.com
qadir
sankaran
van

### Patches

unhandled-XML-exception.patch

Add patch

Ubuntu Foundations Team Bug Bot (crichton) wrote on 2020-05-18: #2

```
The attachment "unhandled-XML-exception.patch" seems to be a patch. If it
isn't, please remove the "patch" flag from the attachment, remove the
"patch" tag, and if you are a member of the ~ubuntu-reviewers, unsubscribe
the team.

[This is an automated message performed by a Launchpad user owned by
~brian-murray, for any issues please contact him.]

tags:added: patch
```

Brian Murray (brian-murray) on 2020-05-18

```
Changed in apport (Ubuntu):
importance:Undecided → Medium
    status:New → Confirmed
```

Seth Arnold (seth-arnold) wrote on 2020-07-14: #3

```
Hello, please use CVE-2020-15701 for this issue. Thanks
```

Launchpad Janitor (janitor) wrote on 2020-08-04: #4

```
This bug was fixed in the package apport - 2.20.11-0ubuntu27.6

---------------
apport (2.20.11-0ubuntu27.6) focal-security; urgency=medium

  * SECURITY UPDATE: information disclosure issue (LP: #1885633)
    - data/apport: also drop gid when checking if user session is closing.
    - CVE-2020-11936
  * SECURITY UPDATE: crash via malformed ignore file (LP: #1877023)
    - apport/report.py: don't crash on malformed mtime values.
    - CVE-2020-15701
  * SECURITY UPDATE: TOCTOU in core file location
    - data/apport: make sure the process hasn't been replaced after Apport
      has started.
    - CVE-2020-15702
  * apport/ui.py, test/test_ui.py: make sure a PID is specified when using
    --hanging (LP: #1876659)
  * WARNING: This package does _not_ contain the changes from
    2.20.11-0ubuntu27.5 in focal-proposed.

 -- Marc Deslauriers <email address hidden> Fri, 31 Jul 2020 09:10:30
-0400

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

Benjamin Drung (bdrung) on 2022-06-27

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

See full activity log

To post a comment you must log in.