

Bugs Blueprints Translations Answers

## Unhandled exception in check ignored()

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

Aff	ects	Status	Importance	Assigned to	Milestone
	Apport	Fix Released	Critical	Unassigned	Apport 2.21.0
	apport (Ubuntu)	Fix Released	Medium	Unassigned	

## **Bug Description**

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

## Description

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

This is an example of apport-ignore.xml

<?xml version="1.0" ?>

<ignore mtime="1461374304" program="/opt/sublime\_text/sublime\_text"/>

<ignore mtime="1453471676" program="/bin/sleep"/</pre>

<ignore mtime="1452699271" program="/usr/bin/strace"/>

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).

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>

File "/usr/lib/python3/dist-packages/apport/report.py", line 1082, in

if float(ignore.getAttribute('mtime')) >= cur mtime:

ValueError: could not convert string to float: 'string'

Sincerely,

See original description

## 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:

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

Ubuntu Review Team

May be notified

Alejandro J. Alva..

Ashani Holland

Benjamin Drung

Brian Murray Bruno Garcia

Charlie Smotherman

Christina A Reitb..

Debian PTS Doraann2

Franko Fano

Hans Christian Holm

HaySayCheese

Hidagawa

Jesse Jones

José Alfonso

Kees Cook

Matt j

Micah Gersten Michael Rowland H...

Mr. MInhai

Name Changed

PCTeacher012

Paolo Tona PechavClub Inc

Peter Bullert

Philip Muškovao

Richard Seguin Richard Williams

Ubuntu Foundation...

Ubuntu Security Team

Ubuntu Touch seed...

Vic Parker

ahepas

basilisgabri dsfkj dfjx

eoininmoran

ganesh linuxgijs

projevie@hotmail.com

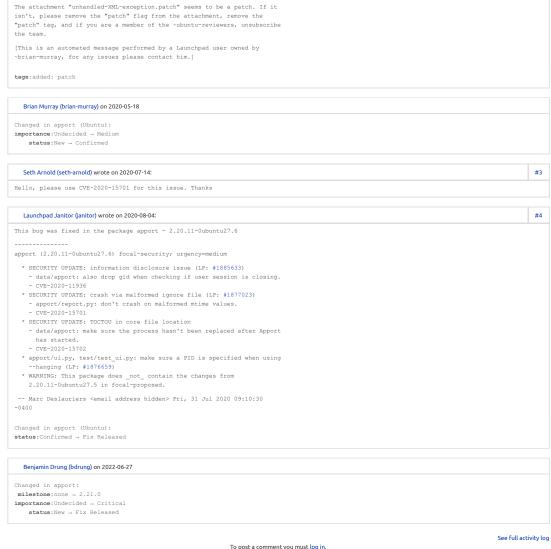
sankaran van

Patches

#1

unhandled-XML-exception.patch

Add patch



To post a comment you must log in.

« Launchpad • Take the tour • Read the guide 
 □

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