Crash in system_server when using RadioTuner::getMetadataImage

+1 Hotlists (2) Mark as Duplicate

Comments (6) Dependencies Duplicates (0) Blocking (0/1) Resources (0)

Obsolete Bug P3 + Add Hotlist [AOSP] assigned

STATUS UPDATE No update yet. Edit

DESCRIPTION gu...@parrot.corp-partner.google.com created issue #1 Jun 1, 2018 08:34PM

android version OPM1.171019.011

When calling RadioTuner::getMetadataImage from an app, I always get a crash in system server (see logcat attached).

Issue comes from nativeGetImage function, from services/core/jni/BroadcastRadio/Tuner.cpp file in the platforms/frameworks/base repo.

This function returns "jRawImage.get();" which cause a call to env->DeleteLocalRef on function exit and consequently a "use after free" in JNI.
Function should instead returns "jRawImage.release();" like done in the nativeGetProgramList function.

When using "jRawImage.release();", crash doesn't occurs anymore and the image is well retrieved by the app.

deleted
0 B

Restricted

COMMENTS All comments ↓ Oldest first

gg...@google.com <gg...@google.com> #2 Jun 5, 2018 05:36PM

Assigned to gg...@google.com.

Can you provide the below requested information to better understand the issue:

Device used
Which device did you use to reproduce this issue?

Steps to reproduce
What steps do others need to take in order to reproduce the issue themselves?

Expected output
What do you expect to occur?

Current output
What do you see instead?

Can please attach the complete bug report.

Android bug report
After reproducing the issue, press the volume up, volume down, and power button simultaneously. This will capture a bug report on your device in the “bug reports” directory. Attach the bug report file to this issue.

Alternate method:
After reproducing the issue, navigate to developer settings, ensure ‘USB debugging’ is enabled, then enable ‘Bug report shortcut’. To take bug report, hold the power button and select the ‘Take bug report’ option.

gu...@parrot.corp-partner.google.com <gu...@parrot.corp-partner.google.com> #3 Jun 5, 2018 10:08PM

I can't add a complete report on a public tracker so I cloned this issue on a private component (see 109720394). You can close this issue as duplicate.

gg...@google.com <gg...@google.com> #4 Jun 8, 2018 05:41PM

We have shared this with our engineering team and will update this issue with more information as it becomes available.

cc...@google.com <cc...@google.com> #5 Jul 30, 2019 12:57PM

Reassigned to vi...@google.com.

assignee changed due to member moving out of team.

sa...@google.com <sa...@google.com> #6 Nov 13, 2019 08:23PM

Reporter	gu...@parrot.corp-partner.go…
Type	Bug
Priority	P3
Severity	S3
Status	Won't fix (Obsolete)
Access	Default access View
Assignee	vi...@google.com
Verifier	--
Collaborators	
CC	gg...@google.com gu...@parrot.corp-partner.google.c
AOSP ID	--
ReportedBy	--
Found In	--
Targeted To	--
Verified In	--
In Prod	

We will be closing this bug as Obsolete. If you still think this issue is reproducible and relevant in the latest Android release (Android Q), please attach a new bug report along with reproduction details. If a reply is not received within the next 14 days, this issue will be closed. Thank you for your understanding.

te...@google.com <te...@google.com> Dec 5, 2019 11:07PM

Status: Won't Fix (Obsolete)