Replicant - Issue #1299

(Yet another) MediaServer vulnerability - CVE-2015-3842

08/18/2015 11:38 PM - My Self

Status:	Closed	**Start date:**	03/30/2015
Priority:	High	**Due date:**	
Assignee:	My Self	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	Any version	**Spent time:**	0.00 hour
Resolution:	fixed	**Grant:**	
Device:		**Type of work:**	

Description

Android versions 2.3 to 5.1.1 should be affected, so Replicant is it, too.
More details:
http://blog.trendmicro.com/trendlabs-security-intelligence/mediaserver-takes-another-hit-with-latest-android-vulnerability/

Solution/Patches
AOSP patch: https://android.googlesource.com/platform/frameworks/av/+/aeea52da00d210587fb3ed895de3d5f2e0264c88

History

#1 - 08/22/2015 07:35 PM - My Self

- File audio-effects-fix-heap-overflow.patch added

I've found a POC app here: https://code.google.com/p/android/issues/detail?id=177610
and tested it on my Replicant (4.2) setup. Surprisingly I can't get my MediaServer to crash with that app, (but it could be I just waited to short, because "the mediaserver component will crash at a random function", the blog says).
Just try it on your own, if you like...

Theoretical Replicant should be affected to that vulnerability, so I strongly recommend to apply the patch "audio-effects-fix-heap-overflow.patch", which is attached.

After merging this patch I've recompiled/reflashed Replicant 4.2 for my device without any misbehavior, and tested the functionalities for several hours, now.
After that I use the POC app again, to check if I could bring the mediaserver component to crash, which wasn't the case, (again).

@everyone: please review the patches and apply it if you like.

#2 - 08/24/2015 08:48 PM - My Self

- % Done changed from 0 to 100

#3 - 08/26/2015 11:39 AM - My Self

- File deleted (audio-effects-fix-heap-overflow.patch)

#4 - 08/26/2015 11:40 AM - My Self

- File audio-effects-fix-heap-overflow.patch added

#5 - 08/30/2015 10:16 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Merged, thanks a lot!

Files

audio-effects-fix-heap-overflow.patch	30.5 KB	08/26/2015	My Self