Replicant - Issue #1251

GraphicBuffer overflow vulnerability - CVE-2015-1474

03/30/2015 03:47 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

I've checked, that Replicant is vulnerable to the GraphicBuffer overflow (bug: 18076253), registered as CVE-2015-1474.
More informations: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1474

Solution/Patch
Android diff: https://android.googlesource.com/platform/frameworks/native/+/38803268570f90e97452cd9a30ac831661829091

History

#1 - 03/30/2015 03:56 PM - My Self

The patch is provided to the mailing list, now: http://lists.osuosl.org/pipermail/replicant/Week-of-Mon-20150330/000666.html

#2 - 07/23/2015 09:56 PM - My Self

- File CVE-2015-1474.patch added

I decided to attach the patch listed above, (and tested with the current Replicant 4.2 sources) on this ticket.
After flashing the patched Replicant, I've tested my productive device several months without any misbehavior.

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

#3 - 08/24/2015 08:49 PM - My Self

- % Done changed from 0 to 100

#4 - 08/26/2015 11:33 AM - My Self

- File deleted (CVE-2015-1474.patch)

#5 - 08/26/2015 11:34 AM - My Self

- File CVE-2015-1474.patch added

#6 - 08/30/2015 10:11 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Merged, thanks a lot!

Files

CVE-2015-1474.patch	2.01 KB	08/26/2015	My Self