Replicant - Issue #1143

broadAnyWhere vulnerability - CVE-2014-8609

12/28/2014 09:22 PM - My Self

Status:	Closed	**Start date:**	12/28/2014
Priority:	High	**Due date:**	
Assignee:	My Self	**% Done:**	0%
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 broadAnyWhere (bug: 17356824), registered as CVE-2014-8609.
More informations: http://seclists.org/fulldisclosure/2014/Nov/81
POC (Proof of Concept): https://www.youtube.com/watch?v=H05-6BoB4ng

Solution
AOSP diff: https://android.googlesource.com/platform/packages/apps/Settings/+/37b58a4
CM commit:
https://github.com/CyanogenMod/android_packages_apps_Settings/commit/0d7a9ae528029b5f767136c238b6beff3f400ea0

History

#1 - 01/17/2015 03:20 PM - Paul Kocialkowski

- Target version changed from 21 to Any version

#2 - 01/18/2015 02:52 PM - My Self

I've tried to modify an existing patch to apply it to the Replicant source code.

I've provided the .patch on the mailing list here:
http://lists.osuosl.org/pipermail/replicant/Week-of-Mon-20150112/000633.html
http://lists.osuosl.org/pipermail/replicant/Week-of-Mon-20150112/000634.html

I've recompiled Replicant 4.2 (with this patch successfully applied before).
After that I've checked that Replicant is not vulnerable anymore to this topic.

#3 - 01/18/2015 02:54 PM - My Self

Wrong links, the right one is: http://lists.osuosl.org/pipermail/replicant/Week-of-Mon-20150112/000635.html

#4 - 01/21/2015 10:10 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Pushed to https://gitorious.org/replicant/packages_apps_settings/commit/08da1c10808a9300683a97d0400655afa6594e83
Thanks!