Replicant - Issue #1683

All Replicant versions from 4.0.3 to 4.4.4 are vulnerable to this ransomware (see details)

04/26/2016 09:17 PM - inge gnue

Status:	Closed	**Start date:**	04/26/2016
Priority:	Urgent	**Due date:**	
Assignee:	Paul Kocialkowski	**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	Any version	**Spent time:**	0.00 hour
Resolution:	duplicate	**Grant:**	
Device:		**Type of work:**	

Description

https://www.bluecoat.com/security-blog/2016-04-25/android-exploit-delivers-dogspectus-ransomware

"Android device in a lab environment was hit with the ransomware when an advertisement containing hostile Javascript loaded from a Web page."

History

#1 - 04/27/2016 12:06 AM - inge gnue

This makes me very concerned about using my Replicant phone at all.

The ideal situation would be an upgrade for all Replicant ports.

So far the only workaround, apart from an upgrade, looks like use of an adblocker or even better a javascript blocker in the browser. That's not to say that the ads couldn't also appear in a non http-browser app hosting ads, but thankfully most F-Droid apps are ad-free.

#2 - 04/27/2016 12:39 AM - inge gnue

F-Droid currently has a few options:

Privacy Browser - a browser that lets you block javascript, cookies, and DOM storage
Tint Browser + Tint Browser Adblock Addon
AdAway for blocking ads within apps
Adblock Plus for blocking ads within apps
Zirco Browser - web browser with ad blocker

And DO NOT browse the web any other way.

#3 - 03/03/2017 02:07 PM - Wolfgang Wiedmeyer

- Status changed from New to Closed

- Resolution set to duplicate

It would be better if you would at least link to an article that describes the actual vulnerability and provides information about patches. If possible, providing the patches directly or linking to them would be the best way to report a security issue.

Looks like this is about the Towelroot vulnerability which was already discussed in #1047.