Replicant - Issue #1023

Fake ID - bug 13678484 & Master Key - bug 10148349 vulnerability

11/06/2014 09:48 AM - My Self

Status:	Closed	**Start date:**	11/06/2014
Priority:	High	**Due date:**	
Assignee:	Paul Kocialkowski	**% 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 hope it's a good idea to open a bug ticket about the forum topic: http://redmine.replicant.us/boards/9/topics/6825

Summary
Replicant seems to be vulnerable to the following two bugs

13678484 (Fake ID)
more informations (on the Readme part if you scroll down): https://github.com/Tungstwenty/FakeIDFix
AOSP patch: https://android.googlesource.com/platform/libcore/+/2bc5e811a817a8c667bca4318ae98582b0ee6dc6

10148349 (Master Key)
more informations: http://www.saurik.com/id/19
AOSP patch: https://android.googlesource.com/platform/libcore/+/8405b26

History

#1 - 11/08/2014 02:47 PM - Denis 'GNUtoo' Carikli

- Category changed from 51 to Security

#2 - 11/08/2014 02:49 PM - Denis 'GNUtoo' Carikli

Does that vulnerability permits to MITM an f-droid application?
For instance if you're downloading an f-droid application trough f-droid,
and that an attacker on the network replaces it with his own while you're download it,
will Replicant/f-droid accept the application?

Or does it only permit an application to access another application's data?

Denis.

#3 - 11/10/2014 11:30 AM - My Self

I don't think that f-droid seems to be the main target. (I don't know, but IMHO[!] open source apps also could include malicious code, if nobody reviews it or initializes a recent code audit).
F-droid don't have to be the only way to get .apk files on your Replicant device. I've seen a lot of open source apps, which provides ready to go .apk files within the github project page for example, (and not every open source app is available in f-droid, too).

The explicit answer of your final question is within this article: https://bluebox.com/blog/technical/android-fake-id-vulnerability/
(Abridgment: apps could manipulate for example the Adobe Systems hardcoded certificate is in the AOSP webkit PluginManager class and so it could leading to a sandbox escape and insertion of malicious code, into other applications, could access NFC hardware used in secure payments, and take device administrative control without any prompt or notification provide to the user of the device).

I've kindly asked bluebox security, if they'll made their free (but proprietary) scanner tools open source, but sadly I didn't got an answer.
I checked Replicant with the <Bluebox Security Scanner> (over a Google Play .apk converter) anyway, and so I verified that Replicant is vulnerable to this two bugs.

#4 - 11/28/2014 09:22 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Everything pushed to the repositories, will be part of the next batch of images.