Replicant - Issue #1311

Android KeyStore Stack Buffer Overflow - CVE-2014-3100

08/21/2015 06:18 PM - My Self

Status:	Rejected	**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:	invalid	**Grant:**	
Device:		**Type of work:**	

Description

Replicant seems not to be affected to the vulnerability, listed here:
http://redmine.replicant.us/boards/39/topics/8283?r=10425#message-10425
More details:
https://securityintelligence.com/android-keystore-stack-buffer-overflow-to-keep-things-simple-buffers-are-always-larger-than-needed/
But why not adding the the "test for keystore crashing"-patch anyway?

Solution/Patches
AOSP patch: https://android.googlesource.com/platform/cts/+/cb35803

History

#1 - 08/22/2015 07:49 PM - My Self

- File CVE-2014-3100.zip added

I've applied the patch "Test-for-keystore-crashing-due-to-malformed-names.patch" to my local Replicant sources.

Additionally I [git add]ed this files to the following path:

- tests/tests/security/src/android/security/cts/KeystoreExploitTest.java
- tests/tests/security/src/android/security/cts/Proc.java

(because of this, I provide this patch as a .zip(ped) patchset "CVE-2014-3100.zip"), which is attached.

Replicant <= 4.2 should not be affected by this vulnerability, but I would recommend to apply this CTS-"test for keystore crashing"-patch, anyway.

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.

@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 11:42 AM - My Self

- File deleted (CVE-2014-3100.zip)

#4 - 08/26/2015 11:42 AM - My Self

- File CVE-2014-3100.zip added

#5 - 08/30/2015 10:19 PM - Paul Kocialkowski

Well, since this only impacts the CTS, it won't benefit users in any way. Since I'd like to keep the diff between Replicant and CM to a minimal, perhaps we could consider dropping this?

#6 - 08/30/2015 10:38 PM - My Self

In consideration of the fact that Replicant (4.2) isn't vulnerable to this (CVE-2014-3100), I could live with the dropping of this (fully CTS related) patch. Well, it was worth an offer :)

#7 - 08/31/2015 03:49 PM - Paul Kocialkowski

- Status changed from New to Rejected

- Resolution set to invalid

Files

CVE-2014-3100.zip	2.96 KB	08/26/2015	My Self