Replicant - Issue #1047

Futex (aka Towelroot) vulnerability - CVE-2014-3153

11/06/2014 10:28 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/6903

Summary
Replicant is (at the moment) vulnerable to the Towelroot security issue.
More informations: http://zomo.herokuapp.com/blog/2014/06/21/pinkie-pies-cve-2014-3153

There seem to exist "android_kernel_samsung_exynos5410" (= AFAIK: Samsung Galaxy S4) patches for CM 11.0:
Main fix:
https://github.com/CyanogenMod/android_kernel_samsung_exynos5410/commit/89bc203bad3b921c6a38a6651b3b46809787d654
Some more (probably optional) fixes:
https://github.com/CyanogenMod/android_kernel_samsung_exynos5410/commit/69e8fe3662e77dd22496314307523c5cd91739e8
https://github.com/CyanogenMod/android_kernel_samsung_exynos5410/commit/5013b860800a0648b996f0a42a5c6aaba03ad06c
https://github.com/CyanogenMod/android_kernel_samsung_exynos5410/commit/11cf6decfdf6b09479caa5b371d32eb5d1b311f2
https://github.com/CyanogenMod/android_kernel_samsung_exynos5410/commit/62a1297de30048e88046348c187613e186580c4a
https://github.com/CyanogenMod/android_kernel_samsung_exynos5410/commit/1e1a82e907b5b9d78b57f0f9576ff46689731ae2

Hope there is an easy way to fix that behavior in Replicant.

History

#1 - 11/08/2014 02:37 PM - Denis 'GNUtoo' Carikli

Maybe we should classify better the security issues.
Here it's a security bug (There is no category for that yet) and it's a privilege escalation.

Is it exploitable by f-droid applications?

Since android applications are somehow sandboxed, would toweelroot work?
It uses mmap, and the sockets API.

- IS mmap prevented?
- Does CONFIG_PARANOID_NETWORK prevent using sockets that way?

Denis.

#2 - 11/08/2014 02:40 PM - Denis 'GNUtoo' Carikli

- Category changed from 51 to Security

#3 - 11/10/2014 11:35 AM - My Self

To f-droid I just could repead, what I've wrote in http://redmine.replicant.us/issues/1023

It seems to work this way: "[...] the app runs some code, the code crashed [sic] android and leave it confused, in its confused state it thinks that the app should be root, then the app installs something to allow other apps to become root."
Source: http://geeksided.com/2014/06/16/towelroot-exploit-reveals-security-nightmare-android/
So it breaks the sandbox and should work unless I'm very much mistaken...

#4 - 11/16/2014 10:47 AM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

This was already fixed in every Replicant kernel, for months now. Please reopen if you find a kernel that doesn't have these patches applied.