Replicant - Issue #1035

Superuser vulnerabilities - CVE-2013-[6768/6769/6770]

11/06/2014 10:09 AM - My Self

Status:	Rejected	**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:	invalid	**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/6837

Summary
Replicant seems to be vulnerable to several security related superuser issues.
More informations: http://forum.xda-developers.com/showthread.php?t=2525552

I only found one single specific patch:
https://plus.google.com/103583939320326217147/posts/YpJaDwsSPsX
But in the changelog are more fixes "CVE-2013-6768, CVE-2013-6769, CVE-2013-6770" listed:
https://play.google.com/store/apps/details?id=com.koushikdutta.superuser

As mentioned by the user: http://redmine.replicant.us/users/1149 it seems to be a good idea to shift the superuser app out from the com.android.settings and use the (updateble) stand alone version from f-droid:
https://f-droid.org/repository/browse/?fdfilter=superuser&fdid=com.koushikdutta.superuser

History

#1 - 11/08/2014 02:41 PM - Denis 'GNUtoo' Carikli

- Category changed from 51 to Security

#2 - 11/08/2014 02:43 PM - Denis 'GNUtoo' Carikli

http://forum.xda-developers.com/showthread.php?t=2525552 says
"Any application" and refers to Android, so I guess we're affected by this privilege escalation vulnerability.

#3 - 11/10/2014 11:33 AM - My Self

I would agree to that.
I still don't know which superuser version is embedded in the Replicant com.android.settings, so I manually (and temporarily) switched to the latest version (1.0.3.0) over the CWM flashable zip file:
http://download.clockworkmod.com/superuser/superuser.zip

#4 - 11/14/2014 02:52 PM - My Self

By the way, I don't know if Replicant is also vulnerable to old(!) "ExynosAbuse" on Exynos4 based device. Replicant supports (for now) the following Exynos 4 Samsung devices:
- Galaxy S 2 (I9100)
- Galaxy Note (N7000)
- Galaxy S 3 (I9300)
- Galaxy Note 2 (N7100)

Could anybody please use the .apk of the following link (with patch informations on the site) to check/verify if Replicant is vulnerable to this root-exploit, too?
http://forum.xda-developers.com/showthread.php?t=2050297

#5 - 11/20/2014 08:56 AM - My Self

Could anybody please use the .apk of the following link (with patch informations on the site) to check/verify if Replicant is vulnerable to this root-exploit, too?
http://forum.xda-developers.com/showthread.php?t=2050297

I've got my I9100 back and could handle it myself. **Replicant 4.2.0002 seems to be <patched> against ExynosAbuse.**
So the focus will stay on Superuser vulnerabilities from above.

#6 - 11/28/2014 07:22 PM - Paul Kocialkowski

- Status changed from New to Rejected

- Resolution set to invalid

This is already fixed in our code: https://gitorious.org/replicant/packages_apps_settings/commit/0deb0104eea19085bc68b42f128b3e9792564abe

Please make sure we are actually affected by a security issue before reporting one next time, by:

1. running exploit code
2. checking whether there is already a fix in the source code if there is no easy exploit