Replicant - Issue #1263

Security revaluation pack [until Android 4.4.3 r1]

04/02/2015 09:54 PM - My Self

Status:	Closed	**Start date:**	04/02/2015
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:	fixed	**Grant:**	
Device:		**Type of work:**	

Description

I've crawled the unofficial changelog script [http://aosp.changelog.to] by using these search criterias:
"CVE"; "secur"ity; "vul"nerability to make a list of the following security patches, which where missing in Replicant 4.2 (for now):

- JDQ39 (4.2.2_r1) to JWR64 (4.3_r0) [http://aosp.changelog.to/aosp-JDQ39-JWR64.html]
  - https://android.googlesource.com/platform/frameworks/base/+/68b13ba
  - https://android.googlesource.com/platform/packages/apps/Phone/+/fff2f9b
    Secure broadcasts, which prevents 3rd party spoofing.
    Bug: 7622253
    Patch-file #1: Bugfix-7622253.patch
    Patch-file #2: Bugfix-7622253-Phone.patch
  - https://android.googlesource.com/platform/frameworks/base/+/a2bdffe
    Prevent SecurityException from crashing Recents
    Bug: 6787477
    Patch-file: Bugfix-6787477.patch
  - https://android.googlesource.com/platform/libcore/+/67ff477
    Fix Security2Test counting
    The test was counting the wrong thing. The alias code path is only triggered by X509 and X.509. This worked when there was only 2 providers that pointed at the opposites. When there were three the problem showed up since it wasn't incrementing the right one.
    Patch-file: Fix-Security2Test-counting.patch
  - https://android.googlesource.com/platform/cts/+/1b08aab
    Add character devices to the insecure devices test.
    Patch-file: Add-char-dvc2insec-dvc-test.patch
  - https://android.googlesource.com/platform/cts/+/96bc825
    BannedFilesTest: Detect devices vulnerable to the cmdclient privilege escalation bug.
    Patch-file: Fix-cmdclient-BannedFilesTest.patch
  - https://android.googlesource.com/platform/packages/apps/Email/+/54c88ff
    Show an error on security exception for attachments.
    This uses an existing notification for bad forwarding. The text is a bit odd ("Attachment not forwarded") but avoids adding new text right now, and at least conveys the error.
    Bug: 8417004
    Patch-file: Bugfix-8417004.patch
  - https://android.googlesource.com/platform/packages/apps/Email/+/5ab92ca
    Ensure security policy notifications are shown
    Bug: 8510828
    Patch-file: Bugfix-8510828.patch

- JDQ39 (4.2.2_r1) to JSS15J (4.3_r2.1) [http://aosp.changelog.to/aosp-JDQ39-JSS15J.html]
  - https://android.googlesource.com/platform/cts/+/deadf91
    Add test for CVE-2013-2094
    Detect CVE-2013-2094, the perf_event_open exploit. A patch for this issue can be found at
    http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8176cced706b5e5d15887584150764894e94e02f
    Bug: 8962304
    Patch-files: CVE-2013-2094.patch
    Additionally please [git] add this files to the following path:
    - tests/tests/security/jni/android_security_cts_NativeCodeTest.cpp
    - tests/tests/security/src/android/security/cts/NativeCodeTest.java
      These two files also includes the following two more Patches:
      - https://android.googlesource.com/platform/cts/+/aa93584

CVE-2013-4254: detect perf_event validate_event bug
Credit: https://github.com/deater/perf_event_tests/blob/master/exploits/arm_perf_exploit.c
More info: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4254
Bug: 11260636
This patch is from the Android diff of: JSS15J (4.3_r2.1) to KRT16M (4.4_r1) - http://aosp.changelog.to/aosp-JSS15J-KRT16M.html

- https://android.googlesource.com/platform/cts/+/ba28fe6
  Add test for CVE-2014-1710.
  Detect devices vulnerable to CVE-2014-1710
  Bug: 13539903
  This patch is from the Android diff of: KOT49H (4.4.2_r1) to KTU84L (4.4.3_r1) - http://aosp.changelog.to/aosp-KOT49H-KTU84L.html
  Patch-package: CVE-2013-2094.zip (containing the files above)

- JSS15J (4.3_r2.1) to KRT16M (4.4_r1) [http://aosp.changelog.to/aosp-JSS15J-KRT16M.html]
  - https://android.googlesource.com/platform/cts/+/ed54695
    AppSecurity: Add traffic stats test, and fix file access test
    Bug: 10349057
    Patch-file: Bugfix-10349057.patch
    - Fix the private file access test which would fail because the path was wrong.
    - Add a test that ensures the private file is actually "not accessible" because it can't be as opposed to it not being there: the new test accesses a public file created at the same time as the private file.
    - Add tests around traffic stats
      - add internet permission to app that creates data.
      - generate private traffic stats (tagged sockets).
      - read back traffic stats to make sure that only public stats are visible.

- KOT49H (4.4.2_r1) to KTU84L (4.4.3_r1) [http://aosp.changelog.to/aosp-KOT49H-KTU84L.html]
  - https://android.googlesource.com/platform/cts/+/0e2d6d9
    CtsVerifier test for lock screen vulnerability fix.
    Lock screen credential reset w/o previous credentials.
    The test asks the user to first set a lock screen password and then launch an intent to change it, using an EXTRA that was not being properly validated before the vulnerability was fixed.
    Bug: 9858403
    Patch-package: Bugfix-9858403.zip (containing the files above)
    Patch-files: Bugfix-9858403.patch
    Additionally please [git] add this files to the following path:
    - apps/CtsVerifier/res/layout/pass_fail_lockconfirm.xml
    - apps/CtsVerifier/src/com/android/cts/verifier/security/LockConfirmBypassTest.java

The only (big) part I've leaved open yet is OpenSSL, which I will provide the next time...

History

#1 - 04/02/2015 11:36 PM - My Self

I've sent the patch files to the mailing list:

- (security-patch-bunch 1/2) http://lists.osuosl.org/pipermail/replicant/Week-of-Mon-20150330/000668.html
- (security-patch-bunch 2/2) http://lists.osuosl.org/pipermail/replicant/Week-of-Mon-20150330/000670.html

#2 - 07/23/2015 10:04 PM - My Self

- File patchset_up_to_4.4.3.zip added

In the meanwhile there where made some changes on the Replicant sources, which makes it necessary to re-adjust the two patch-files:

- Bugfix-7622253.patch and
- Bugfix-7622253-Phone.patch

again. So I decided to attach all the current patches listed above, (and tested with the current Replicant 4.2 sources) on this ticket.
After flashing the patched Replicant, I've tested my productive device several months, (and the 2 re-adjusted patches, several weeks) without any misbehavior.

@everyone: please review the patches and apply them if you like.

#3 - 08/10/2015 01:51 PM - My Self

- File patchset_up_to_4.4.3.zip added

I've revised the "Bugfix-7622253.patch" again, (careless mistake) to fit it to the current codebase.
I've decided to attach the complete patchset again, (hopefully the last time).

PS: Because it was unspoken until now, please respect the order of the single patches, as shown above.
PPS: (for those who doesn't know): to "[git] add" the files, like mentioned above, just copy/move the files in place and use:
git add .
git commit -m "Think of something nice"

Have fun.

#4 - 08/24/2015 08:48 PM - My Self

- % Done changed from 0 to 100

#5 - 08/26/2015 11:59 AM - My Self

- File deleted (patchset_up_to_4.4.3.zip)

#6 - 08/26/2015 12:00 PM - My Self

- File deleted (patchset_up_to_4.4.3.zip)

#7 - 08/26/2015 12:00 PM - My Self

- File patchset_up_to_4.4.3.zip added

#8 - 08/31/2015 03:50 PM - Paul Kocialkowski

- Status changed from New to Closed

- Resolution set to fixed

Merged the bits that don't relate to the CTS, thanks a lot!

Files

patchset_up_to_4.4.3.zip	23.9 KB	08/26/2015	My Self