Replicant - Issue #1395

Nexus Security Bulletin from September

10/18/2015 07:10 PM - Wolfgang Wiedmeyer

Status:	Closed	**Start date:**	10/18/2015
Priority:	High	**Due date:**	
Assignee:	Paul Kocialkowski	**% Done:**	90%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	Replicant 4.2	**Spent time:**	0.00 hour
Resolution:	wontfix	**Grant:**	
Device:			

Description

Same procedure as in #1389. This time the bulletin from September:
https://groups.google.com/forum/?_escaped_fragment_=msg/android-security-updates/1M7qbSvACjo/Y7jewiW1AwAJ#!msg/android-security-updates/1M7qbSvACjo/Y7jewiW1AwAJ

CVE-2015-3636: Elevation of Privilege Vulnerability in Kernel
https://github.com/torvalds/linux/commit/a134f083e79f

Elevation of Privilege Vulnerability in Binder
CVE-2015-3845
https://android.googlesource.com/platform/frameworks/native/+/e68cbc3e9e66df4231e70efa3e9c41abc12aea20%5E!/
CVE-2015-1528
https://android.googlesource.com/platform/frameworks/native/+/7dcd0ec9c91688cfa3f679804ba6e132f9811254%5E!/
https://github.com/CyanogenMod/android_system_core/commit/d869e89766d80256117c528bbcc0854acbc068f1

CVE-2015-3863: Elevation of Privilege Vulnerability in Keystore
https://android.googlesource.com/platform/system/security/+/bb9f4392c2f1b11be3acdc1737828274ff1ec55b%5E!/
merge conflict resolved

CVE-2015-3849: Elevation of Privilege Vulnerability in Region
https://android.googlesource.com/platform/frameworks/base/+/4cff1f49ff95d990d6c2614da5d5a23d02145885%5E!/
merge conflict: Problem is that readFromMemory() is not available in Replicant's Skia, so I kept the unflatten function in there.

https://android.googlesource.com/platform/frameworks/base/+/1e72dc7a3074cd0b44d89afbf39bbf5000ef7cc3%5E!/
merge conflict: Same as above, working around missing readFromMemory()

CVE-2015-3858: Elevation of Privilege vulnerability in SMS enables notification bypass.
It seems that Replicant is not affected by this. android.permission.SEND_SMS_NO_CONFIRMATION was renamed to android.permission.SEND_RESPOND_VIA_MESSAGE in API level 18 so we should be safe.

CVE-2015-3861: Denial of Service Vulnerability in Mediaserver
https://android.googlesource.com/platform/frameworks/av/+/304ef91624e12661e7e35c2c0c235da84a73e9c0%5E!/
merge conflict resolved

History

#1 - 11/18/2015 08:59 PM - My Self

- File sec-bulletin-september-patches-reviewed.zip added

- Status changed from New to In Progress

- % Done changed from 0 to 90

Thanks a lot for providing that patchset!

I've merged them all to my local repo and successfully compiled/reflashed/tested Replicant 4.2 on my i9100.

I've attached your patchset again, with the suffix -reviewed. I've modified the header of your patches inside of this attachment a bit. I added a Signed-off-by: {'From:' contact of the originally patch header}, followed by your Signed-off-by/Tested-by line, finalized with my Tested-by line. Hope that's ok?
Additionally I added one left patch (0009-Externally-reported-Moderate-severity-vulnerability.patch) in that reuploaded patchset.

I've looked through the September patches, provided by Google (https://groups.google.com/forum/#!topic/android-security-updates/1M7qbSvACjo) a bit and completed the overview as follows:

CVE-2015-3864: Remote Code Execution Vulnerability in Mediaserver

ANDROID-23034759: https://android.googlesource.com/platform/frameworks/av/+/6fe85f7e15203e48df2cc3e8e1c4bc6ad49dc968
Affected versions: 5.1 and below
Result: already included in the stagefright patchset: http://redmine.replicant.us/issues/1287

CVE-2015-3636: Elevation of Privilege Vulnerability in Kernel

ANDROID-20770158: https://github.com/torvalds/linux/commit/a134f083e79f
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0001-ipv4-Missing-sk_nulls_node_init-in-ping_unhash.patch

CVE-2015-3845: Elevation of Privilege Vulnerability in Binder

ANDROID-17312693: https://android.googlesource.com/platform/frameworks/native/+/e68cbc3e9e66df4231e70efa3e9c41abc12aea20
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0002-Disregard-alleged-binder-entities-beyond-parcel-boun.patch

CVE-2015-1528: Elevation of Privilege Vulnerability in Binder

ANDROID-19334482:
https://android.googlesource.com/platform/frameworks/native/+/7dcd0ec9c91688cfa3f679804ba6e132f9811254
Result: Included in Wolfgang Wiedmeyer's patchset -> 0003-Verify-that-the-native-handle-was-created.patch
https://android.googlesource.com/platform/system/core/+/e8c62fb484151f76ab88b1d5130f38de24ac8c14
Result: Included in Wolfgang Wiedmeyer's patchset -> 0004-Prevent-integer-overflow-when-allocating-native_hand.patch
Affected versions: 5.1 and below

CVE-2015-3863: Elevation of Privilege Vulnerability in Keystore

ANDROID-22802399: https://android.googlesource.com/platform/system/security/+/bb9f4392c2f1b11be3acdc1737828274ff1ec55b
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0005-Fix-unchecked-length-in-Blob-creation.patch

CVE-2015-3849: Elevation of Privilege Vulnerability in Region

ANDROID-20883006:
https://android.googlesource.com/platform/frameworks/base/+/4cff1f49ff95d990d6c2614da5d5a23d02145885
Result: Included in Wolfgang Wiedmeyer's patchset -> 0006-Check-that-the-parcel-contained-the-expected-amount.patch
https://android.googlesource.com/platform/frameworks/base/+/1e72dc7a3074cd0b44d89afbf39bbf5000ef7cc3
Result: Included in Wolfgang Wiedmeyer's patchset -> 0007-DO-NOT-MERGE-Ensure-that-unparcelling-Region-only-re.patch
Affected versions: 5.1 and below

CVE-2015-3858: Elevation of Privilege vulnerability in SMS enables notification bypass.

ANDROID-22314646: https://android.googlesource.com/platform/frameworks/opt/telephony/+/df31d37d285dde9911b699837c351aed2320b586
Affected versions: 5.1 and below
Result: the patch wasn't found in the patchset, so I **added** it as: **0009-Externally-reported-Moderate-severity-vulnerability.patch**

CVE-2015-3860: Elevation of Privilege Vulnerability in Lockscreen

ANDROID-22214934: https://android.googlesource.com/platform/frameworks/base/+/8fba7e6931245a17215e0e740e78b45f6b66d590
Affected versions: 5.1 and 5.0
Result: codebase checked, not needed on Replicant 4.2.

CVE-2015-3861: Denial of Service Vulnerability in Mediaserver

ANDROID-21296336: https://android.googlesource.com/platform/frameworks/av/+/304ef91624e12661e7e35c2c0c235da84a73e9c0
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0008-Guard-against-codecinfo-overflow.patch

#2 - 12/10/2015 12:09 AM - Wolfgang Wiedmeyer

> Additionally I added one left patch (0009-Externally-reported-Moderate-severity-vulnerability.patch) in that reuploaded patchset.
>
> > CVE-2015-3858: Elevation of Privilege vulnerability in SMS enables notification bypass.
> >
> > ANDROID-22314646: https://android.googlesource.com/platform/frameworks/opt/telephony/+/df31d37d285dde9911b699837c351aed2320b586
> > Affected versions: 5.1 and below
> > Result: the patch wasn't found in the patchset, so I **added** it as: **0009-Externally-reported-Moderate-severity-vulnerability.patch**
>
> Including that patch is imho not a good idea. I already wrote:
>
> > It seems that Replicant is not affected by this. android.permission.SEND_SMS_NO_CONFIRMATION was renamed to >android.permission.SEND_RESPOND_VIA_MESSAGE in API level 18 so we should be safe.
>
> So if this patch is included in the current Replicant 4.2 code, it checks for a permission string that does not exist. This would actually introduce the vulnerability in Replicant.
>
> Please correct me if I'm wrong!

#3 - 12/11/2015 02:52 PM - Denis 'GNUtoo' Carikli

- Device Not device specific added

#4 - 05/30/2016 12:14 PM - My Self

- Device added

- Device deleted (Not device specific)

Wolfgang Wiedmeyer wrote:

> Additionally I added one left patch (0009-Externally-reported-Moderate-severity-vulnerability.patch) in that reuploaded patchset.
>
> > CVE-2015-3858: Elevation of Privilege vulnerability in SMS enables notification bypass.
> >
> > ANDROID-22314646:
> > https://android.googlesource.com/platform/frameworks/opt/telephony/+/df31d37d285dde9911b699837c351aed2320b586
> > Affected versions: 5.1 and below
> > Result: the patch wasn't found in the patchset, so I **added** it as: **0009-Externally-reported-Moderate-severity-vulnerability.patch**
>
> Including that patch is imho not a good idea. I already wrote:
>
> > It seems that Replicant is not affected by this. android.permission.SEND_SMS_NO_CONFIRMATION was renamed to >android.permission.SEND_RESPOND_VIA_MESSAGE in API level 18 so we should be safe.
>
> So if this patch is included in the current Replicant 4.2 code, it checks for a permission string that does not exist. This would actually introduce the vulnerability in Replicant.
>
> Please correct me if I'm wrong!

Sorry, my bad. You're absolutely right.

#5 - 04/22/2017 06:21 PM - Wolfgang Wiedmeyer

- Target version set to Replicant 4.2

#6 - 08/16/2019 08:59 PM - Kurtis Hanna

- Status changed from In Progress to Closed

- Resolution set to wontfix

This issue has been closed because Replicant 4.2 is no longer supported or maintained.

Files

sec-bulletin-september-patches.zip	6.67 KB	10/18/2015	Wolfgang Wiedmeyer

sec-bulletin-september-patches-reviewed.zip	8.99 KB	11/18/2015	My Self