Replicant - Issue #1389

Nexus Security Bulletin from August

10/18/2015 12:59 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

Google now releases monthly security bulletins. I went through the one from August, which also includes some older security fixes:
https://groups.google.com/forum/?_escaped_fragment_=msg/android-security-updates/Ugvu3fi6RQM/yzJvoTVrIQAJ#!msg/android-security-updates/Ugvu3fi6RQM/yzJvoTVrIQAJ
Although most of the Stagefright related stuff is already fixed in Replicant, some other security bugs aren't.
I added a note below the link to the commit if the patch needed to be changed.

CVE-2015-3836: Buffer overflow in Sonivox Parse_wave
https://android.googlesource.com/platform/external/sonivox/+/e999f077f6ef59d20282f1e04786816a31fb8be6%5E!/

CVE-2015-3832: Buffer overflows in libstagefright MPEG4Extractor.cpp
https://github.com/CyanogenMod/android_frameworks_av/commit/c086b29ee1353fe85e3c08cb2ea4ce1f5dd462d7
merge conflict resolved

CVE-2015-0973: Vulnerability in libpng: Overflow in png_Read_IDAT_data
https://github.com/CyanogenMod/android_external_libpng/commit/abd737d8149ee16d843c2d9d65f75ecf13d6ca99

CVE-2015-1863: Remotely exploitable memcpy() overflow in p2p_add_device() in wpa_supplicant
https://android.googlesource.com/platform/external/wpa_supplicant_8/+/4cf0f2d0d869c35a9ec4432861d5efa8ead4279c%5E!/
Replicant also has the repository external_wpa_supplicant_8_ti, so I applied the patch to this repository, too.

CVE-2015-3834: Buffer overflow in mediaserver BnHDCP
https://android.googlesource.com/platform/frameworks/av/+/c82e31a7039a03dca7b37c65b7890ba5c1e18ced%5E!/
merge conflict resolved

CVE-2015-3835: Buffer overflow in libstagefright OMXNodeInstance::emptyBuffer
https://github.com/CyanogenMod/android_frameworks_av/commit/49fa7b75b65c3047f55efb4cd2b25261f4289799

CVE-2015-3843: Applications can intercept or emulate SIM commands to Telephony
https://android.googlesource.com/platform/frameworks/opt/telephony/+/b48581401259439dc5ef6dcf8b0f303e4cbefbe9%5E!/
merge conflict resolved

https://android.googlesource.com/platform/packages/apps/Stk/+/1d8e00160c07ae308e5b460214eb2a425b93ccf7%5E!/
merge conflict resolved

https://android.googlesource.com/platform/frameworks/base/+/a5e904e7eb3aaec532de83ca52e24af18e0496b4%5E!/#F0
merge conflict resolved

CVE-2015-1536: Vulnerability in Bitmap unmarshalling
https://android.googlesource.com/platform/frameworks/base/+/d44e5bde18a41beda39d49189bef7f2ba7c8f3cb%5E!/
patch does not work at all. I ported the changes manually. There is also a small change in external/skia necessary for this patch to work. Please review carefully!

CVE-2015-3844: ActivityManagerService.getProcessRecordLocked() may load a system UID application into the wrong process
https://github.com/CyanogenMod/android_frameworks_base/commit/22a5396c052bef500ceea2522c7d8ae61be39c4f

Patches are attached.
These and my other changes can also be found in my personal repository at https://code.fossencdi.org

History

#1 - 11/17/2015 09:38 PM - My Self

- File sec-bulletin-august-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 line, finalized with my Tested-by line. Hope that's ok?

I've looked through the August patches, provided by Google (https://groups.google.com/forum/#!topic/android-security-updates/Ugvu3fi6RQM) a bit and completed the overview as follows:

CVE-2015-1538: Integer overflows during MP4 atom processing

ANDROID-20139950:
https://android.googlesource.com/platform/frameworks/av/+/cf1581c66c2ad8c5b1aaca2e43e350cf5974f46d
https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469f80dd9a22f1328bc81046398
Affected versions: 5.1 and below
Result: already included in the stagefright patchset: http://redmine.replicant.us/issues/1287

CVE-2015-1539: An integer underflow in ESDS processing

ANDROID-20139950: https://android.googlesource.com/platform/frameworks/av/+/5e751957ba692658b7f67eb03ae5ddb2cd3d970c
Affected versions: 5.1 and below
Result: already included in the stagefright patchset: http://redmine.replicant.us/issues/1287

CVE-2015-3824: Integer overflow in libstagefright when parsing the MPEG4 tx3g atom

ANDROID-20923261: https://android.googlesource.com/platform/frameworks/av/+/463a6f807e187828442949d1924e143cf07778c6
Affected versions: Android 5.1 and below
Result: already included in the stagefright patchset: http://redmine.replicant.us/issues/1287

CVE-2015-3827: Integer underflow in libstagefright when processing MPEG4 covr atoms

ANDROID-20923261: https://android.googlesource.com/platform/frameworks/av/+/f4a88c8ed4f8186b3d6e2852993e063fc33ff231
Affected versions: Android 5.1 and below
Result: already included in the stagefright patchset: http://redmine.replicant.us/issues/1287

CVE-2015-3829: Integer overflow in libstagefright processing MPEG4 covr atoms when chunk_data_size is SIZE_MAX

ANDROID-20923261: https://android.googlesource.com/platform/frameworks/av/+/2674a7218eaa3c87f2ee26d26da5b9170e10f859
Affected versions: Android 5.1 and below
Result: already included in the stagefright patchset: http://redmine.replicant.us/issues/1287

CVE-2015-3828: Integer underflow in libstagefright if size is below 6 while processing 3GPP metadata

ANDROID-20923261: https://android.googlesource.com/platform/frameworks/av/+/f4f7e0c102819f039ebb1972b3dba1d3186bc1d1
Affected versions: Android 5.0 and above
Result: codebase checked, not needed on Replicant 4.2.

CVE-2015-3831: Buffer overflow in mediaserver BpMediaHTTPConnection

ANDROID-19400722: https://android.googlesource.com/platform/frameworks/av/+/51504928746edff6c94a1c498cf99c0a83bedaed
Affected versions: 5.0 and 5.1
Result: codebase checked, not needed on Replicant 4.2.

CVE-2015-3837: Memory Corruption in OpenSSLX509Certificate Deserialization

ANDROID-21437603: https://android.googlesource.com/platform/external/conscrypt/+/edf7055461e2d7fa18de5196dca80896a56e3540

Affected versions: 5.1 and below
Result: codebase checked, not needed on Replicant 4.2.

CVE-2015-1541: AppWidgetServiceImpl can create IntentSender with system privileges

ANDROID-19618745: https://android.googlesource.com/platform/frameworks/base/+/0b98d304c467184602b4c6bce76fda0b0274bc07
Affected versions: 5.1 only
Result: codebase checked, not needed on Replicant 4.2.

CVE-2015-3833: Mitigation bypass of restrictions on getRecentTasks()

ANDROID-20034603: https://android.googlesource.com/platform/frameworks/base/+/aaa0fee0d7a8da347a0c47cef5249c70efee209e
Affected versions: 5.0 and 5.1
Result: codebase checked, not needed on Replicant 4.2.

CVE-2015-3826: Unbounded buffer read in libstagefright while parsing 3GPP metadata

ANDROID-20923261: https://android.googlesource.com/platform/frameworks/av/+/f4f7e0c102819f039ebb1972b3dba1d3186bc1d1
Affected versions: 5.0 and 5.1
Result: codebase checked, not needed on Replicant 4.2.

CVE-2015-3835: Buffer overflow in libstagefright OMXNodeInstance::emptyBuffer

ANDROID-20634516:
https://android.googlesource.com/platform/frameworks/av/+/086d84f45ab7b64d1a7ed7ac8ba5833664a6a5ab
Result: Included in Wolfgang Wiedmeyer's patchset -> 0006-DO-NOT-MERGE-IOMX-Add-buffer-range-check-to-emptyBuf.patch
https://android.googlesource.com/platform/frameworks/av/+/3cb1b6944e776863aea316e25fdc16d7f9962902
Result: codebase checked, not needed on Replicant 4.2.
Affected versions: 5.1 and below

CVE-2015-3843: Applications can intercept or emulate SIM commands to Telephony

ANDROID-21697171:
https://android.googlesource.com/platform/frameworks/opt/telephony/+/b48581401259439dc5ef6dcf8b0f303e4cbefbe9
Result: Included in Wolfgang Wiedmeyer's patchset -> 0007-DO-NOT-MERGE-Change-to-add-STK_PERMISSION-for-stk-re.patch
https://android.googlesource.com/platform/packages/apps/Stk/+/1d8e00160c07ae308e5b460214eb2a425b93ccf7
Result: Included in Wolfgang Wiedmeyer's patchset -> 0008-DO-NOT-MERGE-Change-to-add-STK_PERMISSION-for-stk-re.patch
https://android.googlesource.com/platform/frameworks/base/+/a5e904e7eb3aaec532de83ca52e24af18e0496b4
Result: Included in Wolfgang Wiedmeyer's patchset -> 0009-DO-NOT-MERGE-Change-to-add-STK_PERMISSION-for-stk-re.patch
https://android.googlesource.com/platform/packages/services/Telephony/+/fcb1d13c320dd1a6350bc7af3166929b4d54a456
Result: codebase checked, not needed on Replicant 4.2.
Affected versions: 5.1 and below

CVE-2015-3836: Buffer overflow in Sonivox Parse_wave

ANDROID-21132860: https://android.googlesource.com/platform/external/sonivox/+/e999f077f6ef59d20282f1e04786816a31fb8be6
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0001-DLS-parser-fix-wave-pool-size-check.patch

CVE-2015-3832: Buffer overflows in libstagefright MPEG4Extractor.cpp

ANDROID-19641538: https://android.googlesource.com/platform/frameworks/av/+/d48f0f145f8f0f4472bc0af668ac9a8bce44ba9b
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0002-DO-NOT-MERGE-Add-AUtils-isInRange-and-use-it-to-dete.patch

CVE-2015-0973: Vulnerability in libpng: Overflow in png_Read_IDAT_data

ANDROID-19499430: https://android.googlesource.com/platform/external/libpng/+/dd0ed46397a05ae69dc8c401f5711f0db0a964fa
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0003-Backport-of-fix-for-CVE-2015-0973-to-libpng-1.2.patch

CVE-2015-1863: Remotely exploitable memcpy() overflow in p2p_add_device() in wpa_supplicant

ANDROID-20076874: https://android.googlesource.com/platform/external/wpa_supplicant_8/+/4cf0f2d0d869c35a9ec4432861d5efa8ead4279c
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0004-P2P-Validate-SSID-element-length-before-copying-it.patch

> CVE-2015-3834: Buffer overflow in mediaserver BnHDCP

ANDROID-20222489: https://android.googlesource.com/platform/frameworks/av/+/c82e31a7039a03dca7b37c65b7890ba5c1e18ced
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0005-HDCP-buffer-over-flow-check-DO-NOT-MERGE.patch

> CVE-2015-3842: Heap overflow in mediaserver AudioPolicyManager::getInputForAttr()

ANDROID-21953516: https://android.googlesource.com/platform/frameworks/av/+/aeea52da00d210587fb3ed895de3d5f2e0264c88
Affected versions: 5.1 and below
Already included in the MediaServer patch: http://redmine.replicant.us/issues/1299

> CVE-2015-1536: Vulnerability in Bitmap unmarshalling

ANDROID-19666945: https://android.googlesource.com/platform/frameworks/base/+/d44e5bde18a41beda39d49189bef7f2ba7c8f3cb
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0010-Fix-for-CVE-2015-1536.patch

> CVE-2015-3844: ActivityManagerService.getProcessRecordLocked() may load a system UID application into the wrong process

ANDROID-21669445: https://android.googlesource.com/platform/frameworks/base/+/e3cde784e3d99966f313fe00dcecf191f6a44a31
Affected versions: 5.1 and below
Result: Included in Wolfgang Wiedmeyer's patchset -> 0012-Prevent-system-uid-component-from-running-in-an-app.patch

There is another patch in the patchset: **0011-add-operator-for-SkAutoTDelete.patch**
IMHO this isn't a patch of Google's monthly (August) patch-release. All I've found (with a quick search) is this:
https://github.com/android/platform_external_skia/commit/1790e25e1829ed4091fb149764425df7a3c9c0e0
https://github.com/android/platform_external_skia/commit/4f7ec55f7128e971318adc11f07fc485c4d50bc5
@Wolfgang Wiedmeyer: would you, (or anybody else) provide some more informations about that patch, please?

#2 - 12/09/2015 11:08 PM - Wolfgang Wiedmeyer

> 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 line, finalized with my Tested-by line. Hope that's ok?

Yes, of course!

> There is another patch in the patchset: **0011-add-operator-for-SkAutoTDelete.patch**
> IMHO this isn't a patch of Google's monthly (August) patch-release. All I've found (with a quick search) is this:
> https://github.com/android/platform_external_skia/commit/1790e25e1829ed4091fb149764425df7a3c9c0e0
> https://github.com/android/platform_external_skia/commit/4f7ec55f7128e971318adc11f07fc485c4d50bc5
> **@Wolfgang Wiedmeyer: would you, (or anybody else) provide some more informations about that patch, please?**

You won't find this patch anywhere. As I already wrote:

> There is also a small change in external/skia necessary for this patch to work. Please review carefully!

The security patch for CVE-2015-1536 changes the type of bitmap from SkBitmap* to SkAutoTDelete<SkBitmap>. The problem is that the code expects elements of bitmap to be accessible by the ->() operator and this operator is not supported by the SkAutoTDelete class in Replicant. So I added the operator as it is implemented in later versions of Skia. That's all what the additional patch is doing.

#3 - 12/11/2015 02:53 PM - Denis 'GNUtoo' Carikli

- Device Not device specific added

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

- Device added

- Device deleted (Not device specific)

> You won't find this patch anywhere. As I already wrote:

> > There is also a small change in external/skia necessary for this patch to work. Please review carefully!
>
> The security patch for CVE-2015-1536 changes the type of bitmap from SkBitmap* to SkAutoTDelete<SkBitmap>. The problem is that the code expects elements of bitmap to be accessible by the ->() operator and this operator is not supported by the SkAutoTDelete class in Replicant. So I added the operator as it is implemented in later versions of Skia. That's all what the additional patch is doing.

Sorry, my bad. Of course you're right.

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

- Target version set to Replicant 4.2

#6 - 08/16/2019 09:00 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-august-patches.zip	13.4 KB	10/18/2015	Wolfgang Wiedmeyer
sec-bulletin-august-patches-reviewed.zip	14.8 KB	11/17/2015	My Self