Infeasible Bug P2 + Add Hotlist

STATUS UPDATE No update yet. Edit

DESCRIPTION se...@gmail.com created issue #1 Nov 14, 2019 06:22PM

Dear all,

Recently I found below issue about SELinux restorecon from PackageInstallerService.
Looks like Google Play Store(Finsky) tries to install calculator app and then PackageManager calls restorecon to label it but it's crahsed.

In the PackageManager, build stageDir and set this path for restorcon(), but it occurs system_server crash.

1. build stageDir from this (vmdl~~~~~~.tmp)
http://androidxref.com/9.0.0_r3/xref/frameworks/base/services/core/java/com/android/server/pm/PackageInstallerService.java#638

2. set stageDir path for restorecon
http://androidxref.com/9.0.0_r3/xref/frameworks/base/services/core/java/com/android/server/pm/PackageInstallerService.java#656

Have you guys ever seen this issue?
Abort message says "pthread_mutex_lock called on a destroyed mutex" and __pthread_mutex_lock() is called here.
http://androidxref.com/9.0.0_r3/xref/external/selinux/libselinux/src/regex.c#216

11-10 14:12:36.929 18606 18606 I Finsky : [2] mkv.a(328): Required downloads: [com.google.android.calculator]
11-10 14:12:37.060 18606 18606 I Finsky : [2] mdw.a(9): Downloading patch for com.google.android.calculator:77100103 (adid: com.google.android.calculator , isid: 55xTVBiCTaWNCstw8p_adQ)
11-10 14:12:37.061 18606 18606 I Finsky : [2] jbu.a(5): Duplicate state set for 'com.google.android.calculator' (0). Already in that state
11-10 14:12:37.061 18606 18606 I Finsky : [2] jcn.a(29): Download com.google.android.calculator added to DownloadQueue
11-10 14:12:37.062 18606 18606 I Finsky : [2] jbu.a(3): com.google.android.calculator from 0 to 1.
11-10 14:12:37.066 18606 18606 I Finsky : [2] mkc.a(6): IT: Sent download request for com.google.android.calculator, adid: com.google.android.calculator, isid: 55xTVBiCTaWNCstw8p_adQ
11-10 14:12:37.067 18606 18606 I Finsky : [2] jce.accept(16): Download com.google.android.calculator starting
--- CRASH HAPPENED ---
11-10 14:12:37.127 18606 18606 I Finsky : [2] jcl.onPostExecute(3): Enqueued com.google.android.calculator as content://downloads/my_downloads/30
11-10 14:12:37.127 18606 18606 I Finsky : [2] jbu.a(3): com.google.android.calculator from 1 to 2.
11-10 14:12:37.127 18606 18606 I Finsky : [2] ehs.a(31): Completed 1 account content syncs with 1 successful.
11-10 14:12:37.132 18606 18606 I Finsky : [2] jcn.g(8): com.google.android.calculator: onStart
11-10 14:12:37.138 18606 18606 I Finsky : [2] mja.a(68): Installer: Notifying status update. package=com.google.android.calculator, status=DOWNLOADING

11-10 14:12:37.078 26264 26264 F DEBUG : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
11-10 14:12:37.078 26264 26264 F DEBUG : Revision: '12'
11-10 14:12:37.078 26264 26264 F DEBUG : ABI: 'arm64'
11-10 14:12:37.079 26264 26264 F DEBUG : Timestamp: 2019-11-10 14:12:37-0500
11-10 14:12:37.079 26264 26264 F DEBUG : pid: 2027, tid: 2540, name: Binder:2027_5 >>> system_server <<<
11-10 14:12:37.079 26264 26264 F DEBUG : uid: 1000
11-10 14:12:37.079 26264 26264 F DEBUG : signal 6 (SIGABRT), code -1 (SI_QUEUE), fault addr --------
11-10 14:12:37.080 26264 26264 F DEBUG : Abort message: 'FORTIFY: pthread_mutex_lock called on a destroyed mutex (0x7aa7741010)'
11-10 14:12:37.080 26264 26264 F DEBUG : x0 0000000000000000 x1 00000000000009ec x2 0000000000000006 x3 0000007aaac58af0
11-10 14:12:37.080 26264 26264 F DEBUG : x4 0000000000000000 x5 0000000000000000 x6 0000000000000000 x7 0000000000000038
11-10 14:12:37.080 26264 26264 F DEBUG : x8 00000000000000f0 x9 b9d3dfcc607616c1 x10 0000000000000001 x11 0000000000000000
11-10 14:12:37.080 26264 26264 F DEBUG : x12 ffffffff0fffffbdf x13 000000005dc86124 x14 002934083af11369 x15 0000ba3ed53ecedb
11-10 14:12:37.080 26264 26264 F DEBUG : x16 0000007c20ef78c8 x17 0000007c20ed3d50 x18 0000007aaa722000 x19 00000000000007eb
11-10 14:12:37.080 26264 26264 F DEBUG : x20 00000000000009ec x21 00000000ffffffff x22 0000000000000000 x23 0000007aa7755ad0
11-10 14:12:37.080 26264 26264 F DEBUG : x24 0000000000000000 x25 0000007b809c9a00 x26 0000000000004000 x27 00000000000000d6
11-10 14:12:37.080 26264 26264 F DEBUG : x28 0000000000000000 x29 0000007aaac58b90
11-10 14:12:37.080 26264 26264 F DEBUG : sp 0000007aaac58ad0 lr 0000007c20e850c4 pc 0000007c20e850f0
11-10 14:12:37.313 26264 26264 F DEBUG :
11-10 14:12:37.313 26264 26264 F DEBUG : backtrace:
11-10 14:12:37.313 26264 26264 F DEBUG : #00 pc 00000000000830f0 /apex/com.android.runtime/lib64/bionic/libc.so (abort+160) (BuildId: e584ec83a3322f37c0476c0c5e2ceb6e)
11-10 14:12:37.313 26264 26264 F DEBUG : #01 pc 00000000000e8320 /apex/com.android.runtime/lib64/bionic/libc.so (__fortify_fatal(char const*, ...)+120) (BuildId: e584ec83a3322f37c0476c0c5e2ceb6e)
11-10 14:12:37.313 26264 26264 F DEBUG : #02 pc 00000000000e79c0 /apex/com.android.runtime/lib64/bionic/libc.so

Reporter se...@gmail.com
Type Bug
Priority P2
Severity S2
Status Won't fix (Infeasible)
Access Default access View
Expanded Access
Assignee ad...@google.com
Verifier --
Collaborators
CC ad...@google.com se...@gmail.com
AOSP ID --
ReportedBy --
Found In --
Targeted To --
Verified In --
In Prod

(HandleUsingDestroyedMutex(pthread_mutex_t*, char const*)+52) (BuildId: e584ec83a3322f37c0476c0c5e2ceb6e)
11-10 14:12:37.313 26264 26264 F DEBUG : #03 pc 00000000000e7874 /apex/com.android.runtime/lib64/bionic/libc.so (pthread_mutex_lock+228) (BuildId: e584ec83a3322f37c0476c0c5e2ceb6e)
11-10 14:12:37.313 26264 26264 F DEBUG : #04 pc 000000000000c6f4 /system/lib64/libselinux.so (regex_match+44) (BuildId: 6ddb492f1ca59fc5d0a4011e5678e05c)
11-10 14:12:37.313 26264 26264 F DEBUG : #05 pc 000000000000ad0c /system/lib64/libselinux.so (lookup_all+872) (BuildId: 6ddb492f1ca59fc5d0a4011e5678e05c)
11-10 14:12:37.313 26264 26264 F DEBUG : #06 pc 000000000000a238 /system/lib64/libselinux.so (lookup+20) (BuildId: 6ddb492f1ca59fc5d0a4011e5678e05c)
11-10 14:12:37.313 26264 26264 F DEBUG : #07 pc 0000000000007e0c /system/lib64/libselinux.so (selabel_lookup+40) (BuildId: 6ddb492f1ca59fc5d0a4011e5678e05c)
11-10 14:12:37.313 26264 26264 F DEBUG : #08 pc 0000000000015c64 /system/lib64/libselinux.so (restorecon_sb+92) (BuildId: 6ddb492f1ca59fc5d0a4011e5678e05c)
11-10 14:12:37.313 26264 26264 F DEBUG : #09 pc 0000000000015148 /system/lib64/libselinux.so (selinux_android_restorecon_common+684) (BuildId: 6ddb492f1ca59fc5d0a4011e5678e05c)
11-10 14:12:37.313 26264 26264 F DEBUG : #10 pc 00000000001427a0 /system/lib64/libandroid_runtime.so (android::native_restorecon(_JNIEnv*, _jobject*, _jstring*, int)+88) (BuildId: 7eba0fceac6b77f49e1f3887cda2a728)
11-10 14:12:37.313 26264 26264 F DEBUG : #11 pc 00000000002c2bd4 /system/framework/arm64/boot-framework.oat (art_jni_trampoline+180) (BuildId: 91686ead274bdb34022132d6d418309d029234e2)
11-10 14:12:37.313 26264 26264 F DEBUG : #12 pc 000000000077605c /system/framework/arm64/boot-framework.oat (android.os.SELinux.restorecon+76) (BuildId: 91686ead274bdb34022132d6d418309d029234e2)
11-10 14:12:37.313 26264 26264 F DEBUG : #13 pc 0000000001767754 /system/framework/oat/arm64/services.odex (com.android.server.pm.PackageInstallerService.prepareStageDir+388) (BuildId: ae395a75a952234958c23009620a0123db23c592)
11-10 14:12:37.313 26264 26264 F DEBUG : #14 pc 000000000166b9a4 /system/framework/oat/arm64/services.odex (com.android.server.pm.PackageInstallerSession.open+196) (BuildId: ae395a75a952234958c23009620a0123db23c592)
11-10 14:12:37.313 26264 26264 F DEBUG : #15 pc 000000000176745c /system/framework/oat/arm64/services.odex (com.android.server.pm.PackageInstallerService.openSessionInternal+252) (BuildId: ae395a75a952234958c23009620a0123db23c592)
11-10 14:12:37.313 26264 26264 F DEBUG : #16 pc 00000000017687d4 /system/framework/oat/arm64/services.odex (com.android.server.pm.PackageInstallerService.openSession+52) (BuildId: ae395a75a952234958c23009620a0123db23c592)
11-10 14:12:37.313 26264 26264 F DEBUG : #17 pc 000000000030fe68 /system/framework/arm64/boot-framework.oat (android.content.pm.IPackageInstaller$Stub.onTransact+2616) (BuildId: 91686ead274bdb34022132d6d418309d029234e2)
11-10 14:12:37.313 26264 26264 F DEBUG : #18 pc 000000000082ea9c /system/framework/arm64/boot-framework.oat (android.os.Binder.execTransactInternal+748) (BuildId: 91686ead274bdb34022132d6d418309d029234e2)
11-10 14:12:37.313 26264 26264 F DEBUG : #19 pc 000000000082e688 /system/framework/arm64/boot-framework.oat (android.os.Binder.execTransact+296) (BuildId: 91686ead274bdb34022132d6d418309d029234e2)
11-10 14:12:37.313 26264 26264 F DEBUG : #20 pc 0000000000136334 /apex/com.android.runtime/lib64/libart.so (art_quick_invoke_stub+548) (BuildId: 52544141efa03b62081531056ee23597)
11-10 14:12:37.313 26264 26264 F DEBUG : #21 pc 0000000000144fec /apex/com.android.runtime/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigned int*, unsigned int, art::JValue*, char const*)+244) (BuildId: 52544141efa03b62081531056ee23597)
11-10 14:12:37.313 26264 26264 F DEBUG : #22 pc 00000000004afc18 /apex/com.android.runtime/lib64/libart.so (art::(anonymous namespace)::InvokeWithArgArray(art::ScopedObjectAccessAlreadyRunnable const&, art::ArtMethod*, art::(anonymous namespace)::ArgArray*, art::JValue*, char const*)+104) (BuildId: 52544141efa03b62081531056ee23597)
11-10 14:12:37.313 26264 26264 F DEBUG : #23 pc 00000000004b1064 /apex/com.android.runtime/lib64/libart.so (art::InvokeVirtualOrInterfaceWithVarArgs(art::ScopedObjectAccessAlreadyRunnable const&, _jobject*, _jmethodID*, std::__va_list)+424) (BuildId: 52544141efa03b62081531056ee23597)
11-10 14:12:37.313 26264 26264 F DEBUG : #24 pc 000000000038bccc /apex/com.android.runtime/lib64/libart.so (art::JNI::CallBooleanMethodV(_JNIEnv*, _jobject*, _jmethodID*, std::__va_list)+628) (BuildId: 52544141efa03b62081531056ee23597)
11-10 14:12:37.313 26264 26264 F DEBUG : #25 pc 00000000000d88e0 /system/lib64/libandroid_runtime.so (_JNIEnv::CallBooleanMethod(_jobject*, _jmethodID*, ...)+116) (BuildId: 7eba0fceac6b77f49e1f3887cda2a728)
11-10 14:12:37.313 26264 26264 F DEBUG : #26 pc 000000000015334c /system/lib64/libandroid_runtime.so (JavaBBinder::onTransact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+156) (BuildId: 7eba0fceac6b77f49e1f3887cda2a728)
11-10 14:12:37.313 26264 26264 F DEBUG : #27 pc 000000000004c678 /system/lib64/libbinder.so (android::BBinder::transact(unsigned int, android::Parcel const&, android::Parcel*, unsigned int)+136) (BuildId: 7b475dbd029ed4c3a6e08ffe7df036fa)
11-10 14:12:37.313 26264 26264 F DEBUG : #28 pc 0000000000059408 /system/lib64/libbinder.so (android::IPCThreadState::executeCommand(int)+992) (BuildId: 7b475dbd029ed4c3a6e08ffe7df036fa)
11-10 14:12:37.313 26264 26264 F DEBUG : #29 pc 0000000000058f74 /system/lib64/libbinder.so (android::IPCThreadState::getAndExecuteCommand()+156) (BuildId: 7b475dbd029ed4c3a6e08ffe7df036fa)
11-10 14:12:37.313 26264 26264 F DEBUG : #30 pc 0000000000596f4 /system/lib64/libbinder.so (android::IPCThreadState::joinThreadPool(bool)+108) (BuildId: 7b475dbd029ed4c3a6e08ffe7df036fa)
11-10 14:12:37.313 26264 26264 F DEBUG : #31 pc 000000000007f7ec /system/lib64/libbinder.so (android::PoolThread::threadLoop()+24) (BuildId: 7b475dbd029ed4c3a6e08ffe7df036fa)
11-10 14:12:37.313 26264 26264 F DEBUG : #32 pc 00000000000135f0 /system/lib64/libutils.so (android::Thread::_threadLoop(void*)+328) (BuildId: 0a108e0dee44e7d074243b1dcd1ebb46)
11-10 14:12:37.313 26264 26264 F DEBUG : #33 pc 00000000000c7b8c /system/lib64/libandroid_runtime.so (android::AndroidRuntime::javaThreadShell(void*)+140) (BuildId: 7eba0fceac6b77f49e1f3887cda2a728)
11-10 14:12:37.313 26264 26264 F DEBUG : #34 pc 00000000000e6ce0 /apex/com.android.runtime/lib64/bionic/libc.so (__pthread_start(void*)+36) (BuildId: e584ec83a3322f37c0476c0c5e2ceb6e)
11-10 14:12:37.313 26264 26264 F DEBUG : #35 pc 0000000000084b6c /apex/com.android.runtime/lib64/bionic/libc.so (__start_thread+64) (BuildId: e584ec83a3322f37c0476c0c5e2ceb6e)

Thanks,
SeokGyu HAN

✓ Links (4) Hide all

“http://androidxref.com/9.0.0_r3/xref/frameworks/base/services/core/java/com/android/server/pm/Pack… ” se...@ #1
“http://androidxref.com/9.0.0_r3/xref/frameworks/base/services/core/java/com/android/server/pm/Pack… ” se...@ #1
“http://androidxref.com/9.0.0_r3/xref/external/selinux/libselinux/…” se...@ #1
“For steps to capture a bug report, please refer: https://developer.android.com/studio/debug/bug-report#bugreportdevice” ad...@ #2

COMMENTS All comments ↓ Oldest first

ad...@google.com <ad...@google.com> #2 Nov 14, 2019 06:40PM

Assigned to ad...@google.com.

Thank you for reporting this issue. For us to further investigate this issue, please provide the following additional information:

Steps to reproduce
What steps do others need to take in order to reproduce the issue themselves?

Android build
Which Android build are you using? (e.g. KVT49L)

Device used
Which device did you use to reproduce this issue?

Android bug report (to be captured after reproducing the issue)
For steps to capture a bug report, please refer: https://developer.android.com/studio/debug/bug-report#bugreportdevice

Alternate method
Navigate to “Developer options”, ensure “USB debugging” is enabled, then enable “Bug report shortcut”. Capture bug report by holding the power button and selecting the “Take bug report” option.

Note: Please upload the files to google drive and share the folder to android-bugreport@google.com, then share the link here.

---

ad...@google.com <ad...@google.com> #3 Nov 21, 2019 03:41PM

Please provide the information requested in comment #2 to investigate this further.

---

ad...@google.com <ad...@google.com> #4 Nov 28, 2019 03:34PM

Status: Won't Fix (Infeasible)

We are closing this issue as we don't have enough actionable information. If you are still facing this problem, please open new issue and add the relevant information along with reference to earlier issue.

---

se...@gmail.com <se...@gmail.com> #5 Nov 28, 2019 03:37PM

Ok I'll reopen this issue if I'm facing this problem again. Thanks !