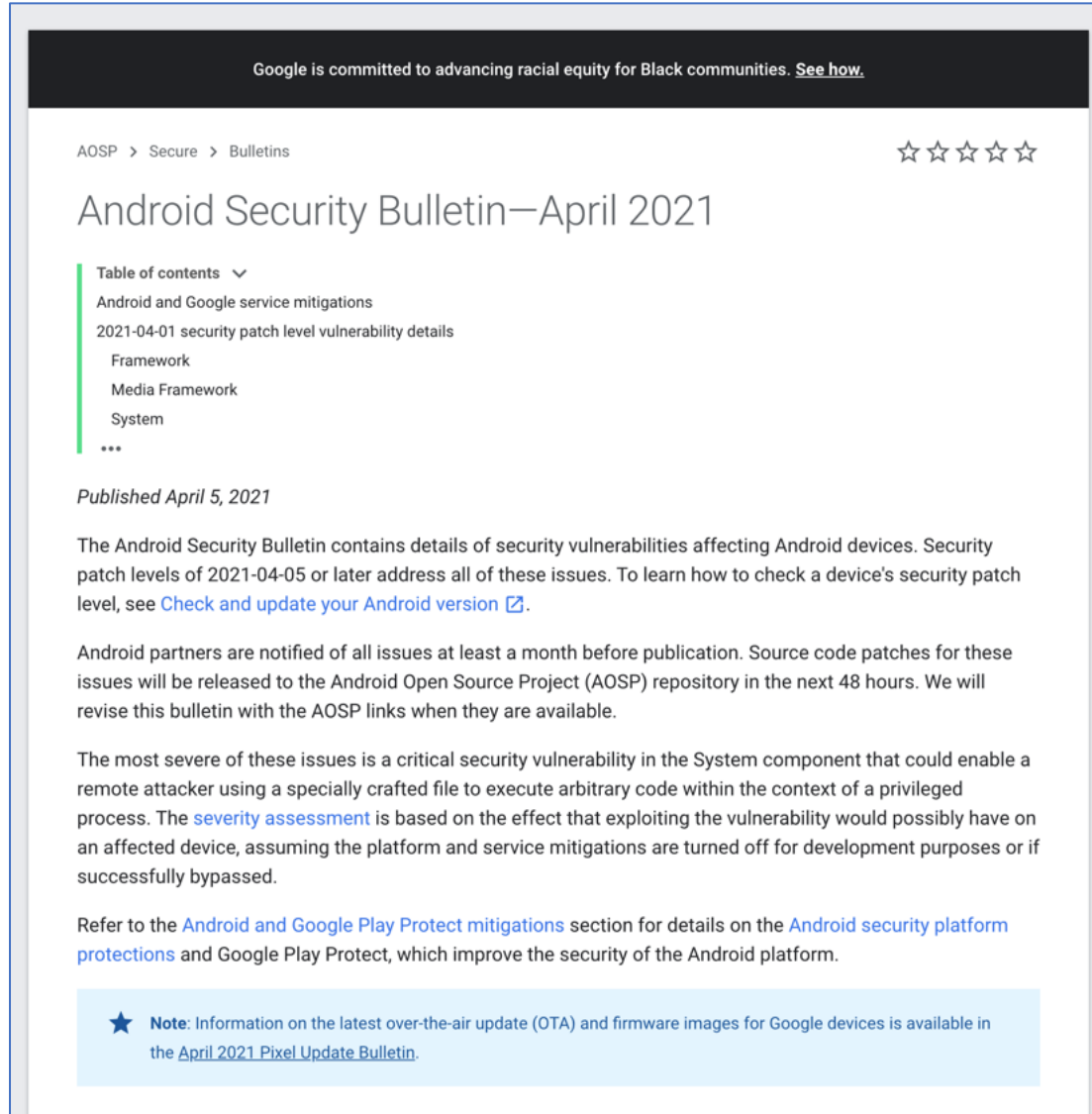


This document shows the details of CVE-2021-0428 and Google's fix as of Apr 2021

(1) Android Security Bulletin – April 2021

(PS. the original webpage has been modified and some information is missing)



Google is committed to advancing racial equity for Black communities. [See how.](#)

AOSP > Secure > Bulletins ☆☆☆☆☆

Android Security Bulletin—April 2021

Table of contents ▾

- Android and Google service mitigations
- 2021-04-01 security patch level vulnerability details
 - Framework
 - Media Framework
 - System
 - ...

Published April 5, 2021

The Android Security Bulletin contains details of security vulnerabilities affecting Android devices. Security patch levels of 2021-04-05 or later address all of these issues. To learn how to check a device's security patch level, see [Check and update your Android version](#).

Android partners are notified of all issues at least a month before publication. Source code patches for these issues will be released to the Android Open Source Project (AOSP) repository in the next 48 hours. We will revise this bulletin with the AOSP links when they are available.

The most severe of these issues is a critical security vulnerability in the System component that could enable a remote attacker using a specially crafted file to execute arbitrary code within the context of a privileged process. The [severity assessment](#) is based on the effect that exploiting the vulnerability would possibly have on an affected device, assuming the platform and service mitigations are turned off for development purposes or if successfully bypassed.

Refer to the [Android and Google Play Protect mitigations](#) section for details on the [Android security platform protections](#) and Google Play Protect, which improve the security of the Android platform.

★ **Note:** Information on the latest over-the-air update (OTA) and firmware images for Google devices is available in the [April 2021 Pixel Update Bulletin](#).

This document shows the details of CVE-2021-0428 and Google's fix as of Apr 2021

(1) Android Security Bulletin – April 2021 (Cont.)

In the bulletin, CVE-2021-0428 was fixed in the 2021-04-05 security patch, with a references **A-173421434**

2021-04-05 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2021-04-05 patch level. Vulnerabilities are grouped under the component they affect. Issues are described in the tables below and include CVE ID, associated references, [type of vulnerability](#), [severity](#), and updated AOSP versions (where applicable). When available, we link the public change that addressed the issue to the bug ID, like the AOSP change list. When multiple changes relate to a single bug, additional references are linked to numbers following the bug ID.

System

The most severe vulnerability in this section could enable a local malicious application to bypass user interaction requirements in order to gain access to additional permissions.

CVE	References	Type	Severity	Updated AOSP versions
CVE-2021-0445	A-172322502	EoP	High	9, 11
CVE-2021-0428	A-173421434	ID	High	10

Kernel components

The most severe vulnerability in this section could enable a local attacker using a specially crafted file to execute arbitrary code within the context of a privileged process.

CVE	References	Type	Severity	Component
CVE-2020-15436	A-174737742 Upstream kernel	EoP	High	Kernel Block Device Subsystem
CVE-2020-25705	A-174737972 Upstream kernel	ID	High	ICMP

(1) Android Security Bulletin – April 2021 (Cont.)

At the end of bulletin, it records the version information as 1.0 (the initial release)

5. What does an * next to the Android bug ID in the References column mean?

Issues that are not publicly available have an * next to the corresponding reference ID. The update for that issue is generally contained in the latest binary drivers for Pixel devices available from the [Google Developer site](#).

6. Why are security vulnerabilities split between this bulletin and device/partner security bulletins, such as the Pixel bulletin?

Security vulnerabilities that are documented in this security bulletin are required to declare the latest security patch level on Android devices. Additional security vulnerabilities that are documented in the device/partner security bulletins are not required for declaring a security patch level. Android device and chipset manufacturers may also publish security vulnerability details specific to their products, such as [Google](#), [Huawei](#), [LGE](#), [Motorola](#), [Nokia](#), or [Samsung](#).

Versions

Version	Date	Notes
1.0	April 5, 2021	Bulletin published.

Was this page helpful?

☆☆☆☆☆

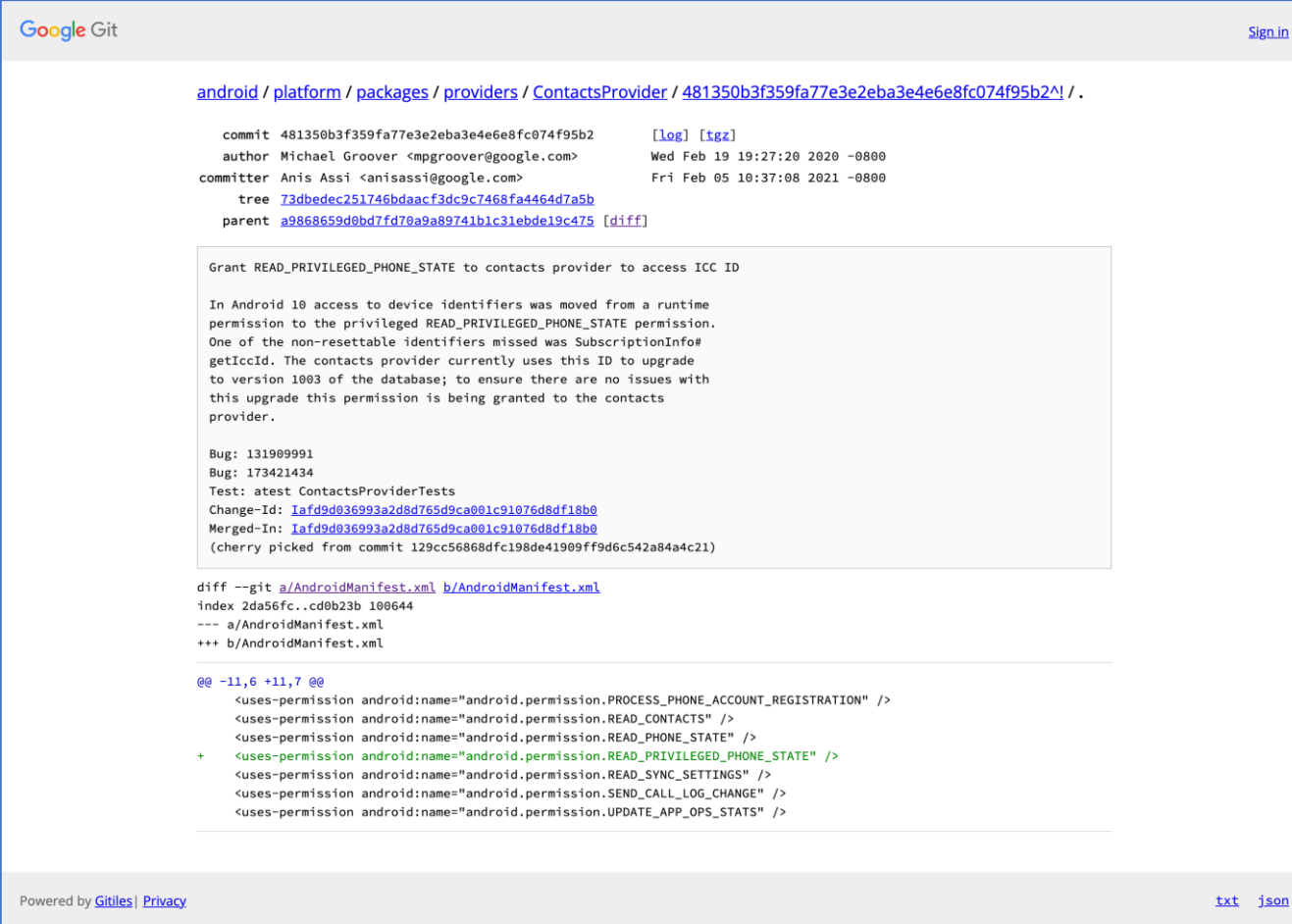
Content and code samples on this page are subject to the licenses described in the [Content License](#). Java is a registered trademark of Oracle and/or its affiliates.

Last updated 2021-04-05 UTC.

Build	Connect	Get help
Android repository	@Android on Twitter	Android Help Center
Requirements	@AndroidDev on Twitter	Pixel Help Center
Downloading	Android Blog	www.android.com
Preview binaries	Google Security Blog	Google Mobile Services
Factory images	Platform on Google Groups	Stack Overflow
Driver binaries	Building on Google Groups	Issue Tracker
GitHub	Porting on Google Groups	

(2) AOSP Repository Git Commit

We search the patch reference **A-173421434** and accordingly locate the chain of commits. From the commit message, we match the fix with the `getIccid()` issue in *SubscriptionInfo* class. We further check another commit that the current one cherry-picks (i.e., **129cc56...**)



Google Git Sign in

[android / platform / packages / providers / ContactsProvider / 481350b3f359fa77e3e2eba3e4e6e8fc074f95b2](#) / .

commit 481350b3f359fa77e3e2eba3e4e6e8fc074f95b2 [\[log\]](#) [\[tgz\]](#)
author Michael Groover <mpgroover@google.com> Wed Feb 19 19:27:20 2020 -0800
committer Anis Assi <anisassi@google.com> Fri Feb 05 10:37:08 2021 -0800
tree [73dbedec251746bdaacf3dc9c7468fa4464d7a5b](#)
parent [a9868659d0bd7fd70a9a89741b1c31ebde19c475](#) [\[diff\]](#)

Grant READ_PRIVILEGED_PHONE_STATE to contacts provider to access ICC ID

In Android 10 access to device identifiers was moved from a runtime permission to the privileged READ_PRIVILEGED_PHONE_STATE permission. One of the non-resettable identifiers missed was SubscriptionInfo.getIccId. The contacts provider currently uses this ID to upgrade to version 1003 of the database; to ensure there are no issues with this upgrade this permission is being granted to the contacts provider.

Bug: 131909991
Bug: 173421434
Test: atest ContactsProviderTests
Change-Id: [Iafd9d036993a2d8d765d9ca01c91076d8df18b0](#)
Merged-In: [Iafd9d036993a2d8d765d9ca01c91076d8df18b0](#)
(cherry picked from commit 129cc56868dfc198de41909ff9d6c542a84a4c21)

```
diff --git a/AndroidManifest.xml b/AndroidManifest.xml
index 2da56fc..cd0b23b 100644
--- a/AndroidManifest.xml
+++ b/AndroidManifest.xml

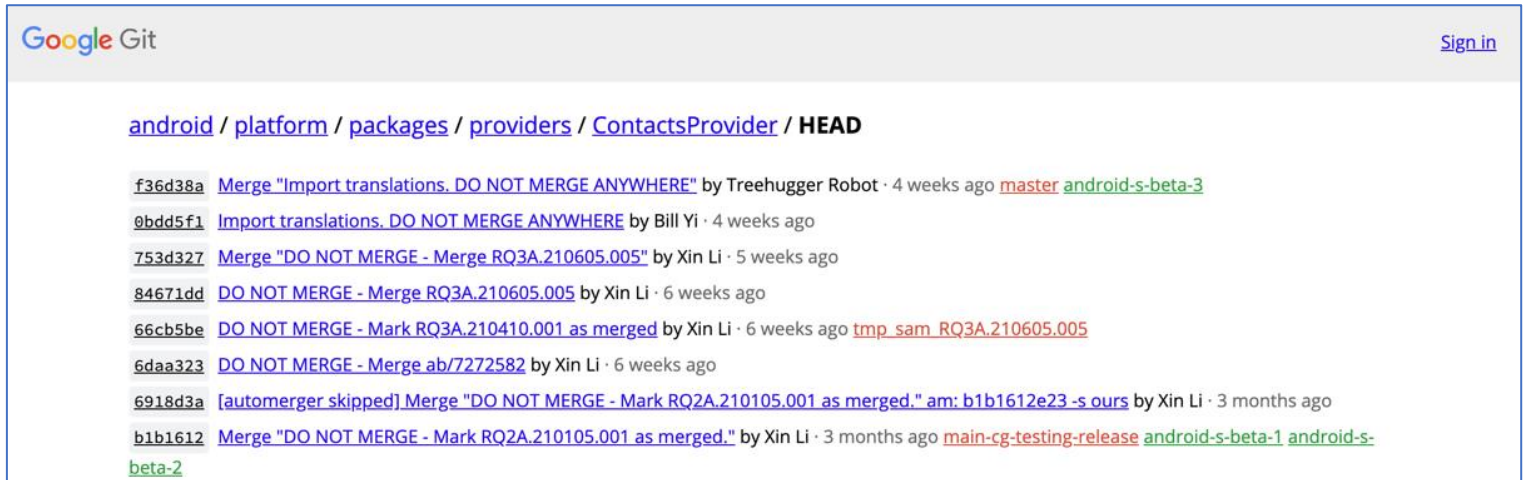
@@ -11,6 +11,7 @@
 <uses-permission android:name="android.permission.PROCESS_PHONE_ACCOUNT_REGISTRATION" />
 <uses-permission android:name="android.permission.READ_CONTACTS" />
 <uses-permission android:name="android.permission.READ_PHONE_STATE" />
+ <uses-permission android:name="android.permission.READ_PRIVILEGED_PHONE_STATE" />
 <uses-permission android:name="android.permission.READ_SYNC_SETTINGS" />
 <uses-permission android:name="android.permission.SEND_CALL_LOG_CHANGE" />
 <uses-permission android:name="android.permission.UPDATE_APP_OPS_STATS" />
```

Powered by [Gitiles](#) | [Privacy](#) [txt](#) [json](#)

This document shows the details of CVE-2021-0428 and Google's fix as of Apr 2021

(2) AOSP Repository Git Commit (Cont.)

Commit history of the ContactsProvider class related to this fix, committed by the same personnel and matched with the same cherry-pick.

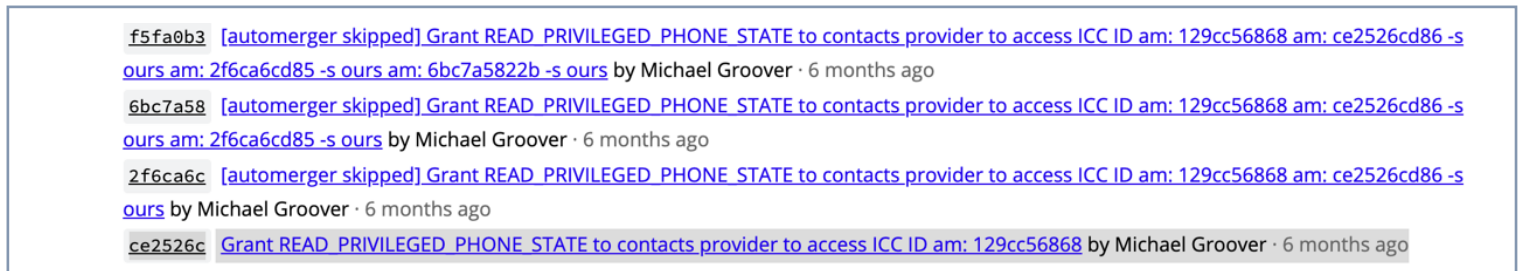


Google Git Sign in

[android](#) / [platform](#) / [packages](#) / [providers](#) / [ContactsProvider](#) / HEAD

- [f36d38a](#) Merge "Import translations. DO NOT MERGE ANYWHERE" by Treehugger Robot · 4 weeks ago [master](#) [android-s-beta-3](#)
- [9bdd5f1](#) Import translations. DO NOT MERGE ANYWHERE by Bill Yi · 4 weeks ago
- [753d327](#) Merge "DO NOT MERGE - Merge RQ3A.210605.005" by Xin Li · 5 weeks ago
- [84671dd](#) DO NOT MERGE - Merge RQ3A.210605.005 by Xin Li · 6 weeks ago
- [66cb5be](#) DO NOT MERGE - Mark RQ3A.210410.001 as merged by Xin Li · 6 weeks ago [tmp_sam](#) [RQ3A.210605.005](#)
- [6daa323](#) DO NOT MERGE - Merge [ab/7272582](#) by Xin Li · 6 weeks ago
- [6918d3a](#) [automerger skipped] Merge "DO NOT MERGE - Mark RQ2A.210105.001 as merged." am: [b1b1612e23](#) -s ours by Xin Li · 3 months ago
- [b1b1612](#) Merge "DO NOT MERGE - Mark RQ2A.210105.001 as merged." by Xin Li · 3 months ago [main-cg-testing-release](#) [android-s-beta-1](#) [android-s-beta-2](#)

↓ scroll down ↓



- [f5fa0b3](#) [automerger skipped] Grant READ_PRIVILEGED_PHONE_STATE to contacts provider to access ICC ID am: 129cc56868 am: [ce2526cd86](#) -s ours am: [2f6ca6cd85](#) -s ours am: [6bc7a5822b](#) -s ours by Michael Groover · 6 months ago
- [6bc7a58](#) [automerger skipped] Grant READ_PRIVILEGED_PHONE_STATE to contacts provider to access ICC ID am: 129cc56868 am: [ce2526cd86](#) -s ours am: [2f6ca6cd85](#) -s ours by Michael Groover · 6 months ago
- [2f6ca6c](#) [automerger skipped] Grant READ_PRIVILEGED_PHONE_STATE to contacts provider to access ICC ID am: 129cc56868 am: [ce2526cd86](#) -s ours by Michael Groover · 6 months ago
- [ce2526c](#) Grant READ_PRIVILEGED_PHONE_STATE to contacts provider to access ICC ID am: [129cc56868](#) by Michael Groover · 6 months ago

The series of commits clearly show that Google added “READ_PRIVILEGED_PHONE_STATE” permission checking in relevant implementation.

This document shows the details of CVE-2021-0428 and Google's fix as of Apr 2021

(3) Commit diff of *SubscriptionInfo* class related to the fix

This diff shows the how Google eventually handled this vulnerability after recalling the fixes in 2021 July. The doc in the comment block says the privileged permission will only be imposed since API level 30 (Android 11).

https://cs.android.com/android/_/android/platform/frameworks/base/+0643914d0573f7084dc86b7b92e2375f962409b2:telephony/java/android/telephony/SubscriptionInfo.java;dlc=a27465258acbc7e4f0007cf2ab3d0cbfd1294893

The screenshot shows the Android Code Search interface with a diff view between two commits: a274652 (left) and 0643914 (right). The file being viewed is telephony/java/android/telephony/SubscriptionInfo.java. The diff highlights changes in the `getNumber()` method and its associated Javadoc comments. In the newer commit (0643914), the Javadoc for `getNumber()` is updated to specify that starting with API level 30, the method returns the ICC ID if the calling app has the `READ_PRIVILEGED_PHONE_STATE` permission, or the ICC ID if the app is a device owner or profile owner with the `READ_PHONE_STATE` permission. The code implementation also reflects this change, returning `mNumber` if the app has the `READ_PHONE_STATE` permission, or an empty string otherwise. The diff uses color coding: green for additions, red for deletions, and yellow for context lines.

```
305 }
306 }
307 /**
308  * Returns the ICC ID if the calling app has been granted the READ_PHONE_STATE
309  * permission, has carrier privileges (see {@link TelephonyManager#hasCarrierPrivileges}),
310  * is a device owner or profile owner that has been granted the READ_PHONE_STATE
311  * permission, or is a device owner or profile owner that owns a managed profile on the
312  * device.
313  * @return the ICC ID, or an empty string if one of these requirements is not met
314  * @deprecated owner access is deprecated and will be removed in a future release
315  */
316 public String getNumber() {
317     return mNumber;
318 }
319
320 /**
321  * Returns the number of this subscription.
322  * Starting with API level 30, returns the number of this subscription if the calling app
323  * has the READ_PHONE_NUMBERS permission, or an empty string otherwise.
324  * @return the number of this subscription, or an empty string if one of these requirements
325  * is not met
326  */
327 public String getNumber() {
328     return mNumber;
329 }
```