Effective in 2026, to align with our trunk stable development model and ensure platform stability for the ecosystem, we will publish source code to AOSP in Q2 and Q4. For building and contributing to AOSP, we recommend utilizing `android-latest-release` instead of `aosp-main`. The `android-latest-release` manifest branch will always reference the most recent release pushed to AOSP. For more information, see Changes to AOSP (/docs/whatsnew/site-updates#aosp-changes).

Android Security Bulletin—April 2026

Published April 6, 2026

This Android Security Bulletin contains details of security vulnerabilities that affect Android devices. Security patch levels of 2026-04-05 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 (https://support.google.com/pixelphone/answer/4457705).

Within 48 hours after the initial publication of this bulletin, we will release the corresponding source code patches to the Android Open Source Project (AOSP) repository. We will then revise this bulletin with the AOSP links.

The most severe of these issues is a critical security vulnerability in the Framework component that could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. The severity assessment (https://source.android.com/security/overview/updates-resources.html#severity) 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.

For more details on the Android security platform protections and Google Play Protect, which improve the security of the Android platform, refer to the Android and Google Play Protect mitigations (#mitigations) section.

We notify our Android partners of all issues at least a month before publishing the bulletin.

Android and Google service mitigations

This is a summary of the mitigations provided by the Android security platform (/security/enhancements) and service protections such as Google Play Protect (https://developers.google.com/android/play-protect). These capabilities reduce the likelihood that security vulnerabilities could be successfully exploited on Android.

- Exploitation for many issues on Android is made more difficult by enhancements in newer versions of the Android platform. We encourage all users to update to the latest version of Android where possible.
- The Android security team actively monitors for abuse through Google Play Protect (https://developers.google.com/android/play-protect) and warns users about Potentially Harmful Applications (/static/security/reports/Google_Android_Security_PHA_classifications.pdf). Google Play Protect is enabled by default on devices with Google Mobile Services (http://www.android.com/gms), and is especially important for users who install apps from outside of Google Play.

2026-04-01 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2026-04-01 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 (#type), severity (/security/overview/updates-resources#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. Devices with Android 10 and later may receive security updates as well as Google Play system updates (https://support.google.com/android/answer/7680439).

Framework

The vulnerability in this section could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.

CVE	References	Type	Severity	Updated AOSP versions
CVE-2026-0049	A-456471290	DoS	Critical	14, 15, 16, 16-qpr2

Google Play system updates

There are no security issues addressed in Google Play system updates (Project Mainline) this month.

2026-04-05 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2026-04-05 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 (#type), severity (/security/overview/updates-resources#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.

Google

This vulnerability affects Google components and further details are available directly from Google. The severity assessment of this issue is provided directly by Google.

CVE	References	Severity	Subcomponent
CVE-2025-48651	A-434039170 * (#asterisk)	High	StrongBox

NXP components

This vulnerability affects NXP components and further details are available directly from NXP. The severity assessment of this issue is provided directly by NXP.

CVE	References	Severity	Subcomponent
CVE-2025-48651	A-467765081 * (#asterisk)	High	StrongBox

STMicroelectronics

This vulnerability affects STMicroelectronics components and further details are available directly from STMicroelectronics. The severity assessment of this issue is provided directly by STMicroelectronics.

CVE	References	Severity	Subcomponent
CVE-2025-48651	A-467765894 * (#asterisk)	High	StrongBox

Thales

This vulnerability affects Thales components and further details are available directly from Thales. The severity assessment of this issue is provided directly by Thales.

CVE	References	Severity	Subcomponent
CVE-2025-48651	A-467762899 * (#asterisk)	High	StrongBox

Common questions and answers

This section answers common questions that may occur after reading this bulletin.

1. How do I determine if my device is updated to address these issues?

To learn how to check a device's security patch level, see Check and update your Android version (https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices).

- Security patch levels of 2026-04-01 or later address all issues associated with the 2026-04-01 security patch level.
- Security patch levels of 2026-04-05 or later address all issues associated with the 2026-04-05 security patch level and all previous patch levels.

Device manufacturers that include these updates should set the patch string level to:

- [ro.build.version.security_patch]:[2026-04-01]
- [ro.build.version.security_patch]:[2026-04-05]

For some devices on Android 10 or later, the Google Play system update will have a date string that matches the 2026-04-01 security patch level. Please see this article (https://support.google.com/android/answer/7680439) for more details on how to install security updates.

2. Why does this bulletin have two security patch levels?

This bulletin has two security patch levels so that Android partners have the flexibility to fix a subset of vulnerabilities that are similar across all Android devices more quickly. Android partners are encouraged to fix all issues in this bulletin and use the latest security patch level.

- Devices that use the 2026-04-01 security patch level must include all issues associated with that security patch level, as well as fixes for all issues reported in previous security bulletins.
- Devices that use the security patch level of 2026-04-05 or newer must include all applicable patches in this (and previous) security bulletins.

Partners are encouraged to bundle the fixes for all issues they are addressing in a single update.

3. What do the entries in the *Type* column mean?

Entries in the *Type* column of the vulnerability details table reference the classification of the security vulnerability.

Abbreviation	Definition
RCE	Remote code execution
EoP	Elevation of privilege
ID	Information disclosure
DoS	Denial of service
N/A	Classification not available

4. What do the entries in the *References* column mean?

Entries under the *References* column of the vulnerability details table may contain a prefix identifying the organization to which the reference value belongs.

Prefix	Reference
A-	Android bug ID
QC-	Qualcomm reference number
M-	MediaTek reference number
N-	NVIDIA reference number
B-	Broadcom reference number
U-	UNISOC reference number

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 (https://developers.google.com/android/drivers).

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 (https://source.android.com/security/bulletin/pixel), Huawei (https://consumer.huawei.com/en/support/bulletin/), LGE (https://lgsecurity.lge.com/security_updates_mobile.html), Motorola (https://motorola-global-portal.custhelp.com/app/software-security-page/g_id/6806), Nokia (https://www.nokia.com/phones/en_int/security-updates), or Samsung (https://security.samsungmobile.com/securityUpdate.smsb).

Versions

Version	Date	Notes
1.0	April 6, 2026	Bulletin published

Last updated 2026-04-06 UTC.