

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—March 2026

Published March 2, 2026 | Updated April 2, 2026

This Android Security Bulletin contains details of security vulnerabilities that affect Android devices. Security patch levels of 2026-03-05 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>).

Source code patches for these issues have been released to the Android Open Source Project (AOSP) repository and linked from this bulletin. This bulletin also includes links to patches outside of AOSP.

The most severe of these issues is a critical security vulnerability in the System component that could lead to remote code execution 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.

Note: There are indications that CVE-2026-21385 may be under limited, targeted exploitation.

2026-03-01 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2026-03-01 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) (https://support.google.com/android/answer/7680439).

Framework

The most severe vulnerability in this section could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

CVE References	Type	Severity	Update AOSP version
CVE- A-465136263 2026- 0047	EoP	Critical	16-qpr
CVE- A-399155883 (https://android.googlesource.com/platform/frameworks/base/+59c15187e7ee299592c22a166528fb27b3a03867) 2025- 32313	EoP	High	14, 15,
CVE- A-415783046 2025- (https://android.googlesource.com/platform/packages/providers/MediaProvider/+a5f1f182733953ef5919311d3d8d2087d9451f1f) 48544	EoP	High	14, 15,
CVE- A-377888957 2025- (https://android.googlesource.com/platform/packages/providers/MediaProvider/+237fb89f532504aeeef0c3ee2038aad89a8a66180) 48567	EoP	High	14, 15,
CVE- A-322157041 2025- 48568	EoP	High	14, 15
CVE- A-428700812 (https://android.googlesource.com/platform/frameworks/base/+1cfd8237b5a8e9fa64367e3d0dff525d63821e1) 2025- 48574	EoP	High	14, 15,
CVE- A-418225717 2025- (https://android.googlesource.com/platform/packages/providers/MediaProvider/+7ea0a039ec32fcd6477355431b953f4689a2fa61) 48578	EoP	High	14, 15,
CVE- A-417195606 2025- (https://android.googlesource.com/platform/packages/providers/MediaProvider/+7ea0a039ec32fcd6477355431b953f4689a2fa61) 48579	EoP	High	14, 15,
CVE- A-369105011 2025- (https://android.googlesource.com/platform/packages/providers/MediaProvider/+1b7d4ce446d149a34d8b317d41127379f017165d) 48582	EoP	High	14, 15,
CVE- A-414387646 (https://android.googlesource.com/platform/frameworks/base/+31e77d73c5e6439bc942a92676c4076ebd8295ff) 2025- 48619	EoP	High	14, 15,
CVE- A-406243581 (https://android.googlesource.com/platform/frameworks/base/+d550a457e65ccbbf252ec2e60d93e8bcd111de0e) 2025- 48634	EoP	High	14, 15,
CVE- A-446678690 2025-	EoP	High	14, 15

48635

CVE- A-443062265 (https://android.googlesource.com/platform/frameworks/base/+cee45869c491d4e39877918ee881eb60dec7d6e5) 2025- 48645	EoP	High	14, 15, 16-qpr
CVE- A-457742426 (https://android.googlesource.com/platform/frameworks/base/+c148b4fae6347652231d1c4a633f5cc9a8f057f8) 2025- 48646	EoP	High	14, 15, 16-qpr
CVE- A-442392902 (https://android.googlesource.com/platform/frameworks/base/+924df83d73d9f938fde025c2e793ca12646207e0) 2025- 48654	EoP	High	16, 16- qpr2
CVE- A-433251166 (https://android.googlesource.com/platform/frameworks/native/+8ec74c568b5881901cad0f1147fdc607702101e0) 2026- 0007	EoP	High	14, 15,
CVE- A-379695596 (https://android.googlesource.com/platform/frameworks/av/+ebdbf918dd87127eaeca15336c33e1d3c1ae7dd6) 2026- 0010	EoP	High	14, 15,
CVE- A-454062218 (https://android.googlesource.com/platform/frameworks/base/+51368785bd09cd652ed9851727b16545cb92c4e5) 2026- 0011	EoP	High	14, 15, 16-qpr
CVE- A-447135012 (https://android.googlesource.com/platform/packages/apps/DocumentsUI/+9f2d3f09f8fdc099d5a2d4c8bf3e8ec460bb9233) 2026- 0013	EoP	High	14, 15,
CVE- A-453649815 (https://android.googlesource.com/platform/frameworks/base/+e770e9f0234158f4631c7147b64a1d70e0843d0b) 2026- 0020	EoP	High	14, 15, 16-qpr
CVE- A-459461121 (https://android.googlesource.com/platform/frameworks/base/+09055276288a68cf35b0f84ba32e28822f74ecf9) 2026- 0023	EoP	High	14, 15, 16-qpr
CVE- A-321711213 2026- 0026	EoP	High	14
CVE- A-428701593 (https://android.googlesource.com/platform/frameworks/base/+e363f82104566378b4b9936d6caf27c3ee631d80) 2026- 0034	EoP	High	14, 15, 16-qpr
CVE- A-455563813 (https://android.googlesource.com/platform/frameworks/native/+c81cf361489e3a3cd764c0a0c85c84958e25d63c) 2025- 48630	ID	High	14, 15, 16-qpr
CVE- A-392614656 (https://android.googlesource.com/platform/frameworks/base/+ef2a8e20316405ce6b704e800b1808c3aaf5ee43) 2026- 0012	ID	High	14, 15,
CVE- A-433746973 (https://android.googlesource.com/platform/frameworks/base/+014dea279c49d532bc4fbbdebbc024133967b6a8) 2026- 0025	ID	High	14, 15, 16-qpr

CVE- A-449181366 (https://android.googlesource.com/platform/frameworks/base/+2bca2265ff3e26b09f9b31c31063147a94e4c5aa) [2] 2025- (https://android.googlesource.com/platform/frameworks/base/+a438ce172b441c8297eadd8d990ab292f5aa7d1)] 48644	DoS	High	14, 15, 16-qpr
CVE- A-443742082 (https://android.googlesource.com/platform/frameworks/base/+b51a58ec96558e1c6b1d47728f45a8795dc7ab) 2026- 0014	DoS	High	14, 15, 16-qpr
CVE- A-445917646 (https://android.googlesource.com/platform/frameworks/base/+a4523e227733ae20eafe4ec3e85474a5b7ebf7c6) 2026- 0015	DoS	High	14, 15, 16-qpr

System

The most severe vulnerability in this section could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

CVE References	Type	Severity	AV
CVE- A-423894847 (https://android.googlesource.com/platform/external/libopenapv/+cf0a0e7a810e5a0f6e50f433c1d723b12160e8dd) [2] 2026- (https://android.googlesource.com/platform/external/libopenapv/+86a76fd73bf7636af018331d4419eaa56ca95083)] [3] 0006 (https://android.googlesource.com/platform/external/libopenapv/+c81fcd419c489dd4aa9efd0ed41fb6c38f853b4f)]	RCE	Critical	1
CVE- A-444671303 (https://android.googlesource.com/platform/frameworks/base/+d6df825fda3aa29cff7af05357005322152210fd) 2025- 48631	DoS	Critical	1
CVE- A-413380719 (https://android.googlesource.com/platform/frameworks/base/+78760f098fab75ae8e952978768d3c7df6312dbd) 2025- 48577	EoP	High	1
CVE- A-407562568 (https://android.googlesource.com/platform/frameworks/base/+c69e16c3efda87ee6435184949549b2f088589b3) 2025- 48602	EoP	High	1
CVE- A-392699284 (https://android.googlesource.com/platform/hardware/st/nfc/+c6da9eeb710c6690d189cb2d1b80b44755860b55) 2025- 48641	EoP	High	1
CVE- A-388530367 (https://android.googlesource.com/platform/packages/providers/TelephonyProvider/+0d45a6a15770ca3ec5d0d2264983c057aae41939) 2025- 48650	EoP	High	1
CVE- A-444673089 (https://android.googlesource.com/platform/packages/apps/Settings/+7d8fbee887fc9577337c2a80513ae4399bf60111) [2] 2026- (https://android.googlesource.com/platform/frameworks/base/+cea235f00865ff73344f1efa9494e47beecc3fd5)] 0017	EoP	High	1 c
CVE- A-430047417 (https://android.googlesource.com/platform/packages/apps/Settings/+48af8a13dd12ecbd0569c328a56d1a7b61a59ca3) 2026- 0021	EoP	High	1 1
CVE- A-418773439 (https://android.googlesource.com/platform/packages/providers/MediaProvider/+119013a3d7e8f1eab671bce4c6a85748752081ed) 2026- 0035	EoP	High	1 1

CVE- A-288144143 2024- (https://android.googlesource.com/platform/packages/modules/Bluetooth/+7ccb456f6d29cc6077a4d1c6a9b515033378ec32) [2] 43766 (https://android.googlesource.com/platform/packages/modules/Bluetooth/+769a3dea8016dd84bea05405d1d5c974755fdb21)	ID	High	1
CVE- A-455777515 2025- (https://android.googlesource.com/platform/packages/modules/Virtualization/+f0271f36388ec9630d89ff8b3ee4cb22e2ca3eaf) 48642	ID	High	1 1
CVE- A-483074175 (https://android.googlesource.com/platform/external/dng_sdk/+6b5cf2a88ebd2b099e56d0d4717e962772ff9067) 2025- 64783	ID	High	1 1
CVE- A-483074618 (https://android.googlesource.com/platform/external/dng_sdk/+6b5cf2a88ebd2b099e56d0d4717e962772ff9067) 2025- 64784	ID	High	1 1
CVE- A-483075215 (https://android.googlesource.com/platform/external/dng_sdk/+6b5cf2a88ebd2b099e56d0d4717e962772ff9067) 2025- 64893	ID	High	1 1
CVE- A-366405211 (https://android.googlesource.com/platform/frameworks/base/+92b109b6041452f6e713dce512fa8de18556360) 2026- 0005	ID	High	1
CVE- A-326211886 2026- (https://android.googlesource.com/platform/packages/providers/MediaProvider/+69a25763cdb46c8f23fe9eb976132acbe2af82d6) 0024	ID	High	1 1
CVE- A-425360742 (https://android.googlesource.com/platform/packages/modules/Profiling/+1215317dfc1d88a4b5ea47185fb8f10afd1f78b0) 2025- 48585	DoS	High	1
CVE- A-425360073 2025- (https://android.googlesource.com/platform/packages/modules/Profiling/+ceaaf1330d3a0697e52691d223ee700824a5b4fa) 48587	DoS	High	1
CVE- A-414388731 2025- (https://android.googlesource.com/platform/packages/providers/TelephonyProvider/+37babc702849821595634b6ecfda6f04404e2cf1) 48609	DoS	High	1

Google Play system updates

The following issues are included in Project Mainline components.

Subcomponent	CVE
Documents UI	CVE-2026-0013
MediaProvider	CVE-2025-48544, CVE-2025-48567, CVE-2025-48578, CVE-2025-48579, CVE-2025-48582
Media Codecs	CVE-2026-0006
MediaProvider	CVE-2026-0024, CVE-2026-0035

Profiling

CVE-2025-48585, CVE-2025-48587

2026-03-05 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2026-03-05 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.

Kernel

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

CVE	References	Type	Severity	Subcomponent
CVE-2024-43859	A-455892000 Upstream kernel (https://android.googlesource.com/kernel/common/+7f97e742f769557693fcf14bd5c1fa06c9478320) [2] (https://android.googlesource.com/kernel/common/+5f04969136db674f133781626e0b692c5f2bf2f0)	EoP	Critical	Flash-Friendly File System
CVE-2026-0037	A-440584506 Upstream kernel (https://android.googlesource.com/kernel/common/+6c400c2e2e46f3a1117ce5da316ecdc1dbb1a031)	EoP	Critical	Protected Kernel-Based Virtual Machine
CVE-2026-0038	-459479964 Upstream kernel (https://android.googlesource.com/kernel/common/+652b7b6bf9a62cc12c3a071bab4e92314f046739) [2] (https://android.googlesource.com/kernel/common/+f090d4b083a9ef4831f99e692c239542dd385cb4) [3] (https://android.googlesource.com/kernel/common/+7e1d15d29b7fe0f858926a8bc9f29b75db9e52a) [4] (https://android.googlesource.com/kernel/common/+b23a5bfa1fb8f9525e21f095a87486a2bd856321) [5] (https://android.googlesource.com/kernel/common/+513ea99ae008b81dd266bf6e361627c058dde41) [6] (https://android.googlesource.com/kernel/common/+1bf8033b56a45165602f8116e0a0d2e767f1e8ae) [7] (https://android.googlesource.com/kernel/common/+d884f499434c224285c30d460681f1ce76a8cf1f)	EoP	Critical	Hypervisor
CVE-2025-38616	A-440544812 Upstream kernel (https://android.googlesource.com/kernel/common/+f1fe99919f629f980d0b8a7ff16950bffe06a859) [2] (https://android.googlesource.com/kernel/common/+eb0336f213fe88bbdb7d2b19c9c9ec19245a3155)	EoP	High	Transport Layer Security
CVE-2025-38618	A-439253642 Upstream kernel (https://android.googlesource.com/kernel/common/+f6266e6d89233aa417e1c684c10102ef1b966ee5) [2] (https://android.googlesource.com/kernel/common/+1ccd273c6de4baef8a0a70971bfa3c8e69fc71d9) [3] (https://android.googlesource.com/kernel/common/+31fc378e731204bbc3a556beb8e10d2a46e4c774)	EoP	High	vsock
CVE-2025-39682	A-440544511 Upstream kernel (https://android.googlesource.com/kernel/common/+2902c3ebcca52ca845c03182000e8d71d3a5196f) [2] (https://android.googlesource.com/kernel/common/+74715c47d57ccbff2f2f00bb9d87288e10642325) [3] (https://android.googlesource.com/kernel/common/+3439c15ae91a517cf3c650ea15a8987699416ad9)	EoP	High	Transport Layer Security

CVE-2025-39946	A-446648770 Upstream kernel (https://android.googlesource.com/kernel/common/+1257aa4519ee5d49e465b0dcc85cc7e4a24619d5) [2] (https://android.googlesource.com/kernel/common/+c4bcbf924ba0823fcdc960c02e0409dbcd345a50)] [3] (https://android.googlesource.com/kernel/common/+8f4e429a1e36e588f434772dceca9068dc1208cc)	EoP	High	Transport Layer Security
CVE-2026-0029	A-443668075 Upstream kernel (https://android.googlesource.com/kernel/common/+ae242b26371808a221578b89c937568781719d2c) [2] (https://android.googlesource.com/kernel/common/+42eff3b2fd3a906ac8cdb6284d3265bc0856b56b)] [3] (https://android.googlesource.com/kernel/common/+749cf1743eb22eff1851c68a533147e1af97a9bf)	EoP	High	Protected Kernel-Based Virtual Machine

Kernel components

The most severe vulnerability in this section could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.

CVE	References	Type	Severity	Subcomponent
CVE-2026-0027	A-456069704 Upstream kernel (https://android.googlesource.com/kernel/common/+3af14d2057f2f3df97472cef6b293113b020d1e6) [2] (https://android.googlesource.com/kernel/common/+a47e0e78ad5b4e153b40fc1c9def11991aa6ca0c)] [3] (https://android.googlesource.com/kernel/common/+5161b3e75fb025bb4ebb11fb1ac037021e56719)	EoP	Critical	Protected Kernel-Based Virtual Machine
CVE-2026-0028	A-443123065 Upstream kernel (https://android.googlesource.com/kernel/common/+986614312222d4b3bdcf16840cdb4abdaed8a42d)] [2] (https://android.googlesource.com/kernel/common/+aff2255dbe38dc7c57bac8d3ba9feed989289b20)] [3] (https://android.googlesource.com/kernel/common/+f3a4b4d4a1fe2aface7de74ac257b8705b6de472)]	EoP	Critical	pKVM
CVE-2026-0030	A-441808375 Upstream kernel (https://android.googlesource.com/kernel/common/+986614312222d4b3bdcf16840cdb4abdaed8a42d)] [2] (https://android.googlesource.com/kernel/common/+aff2255dbe38dc7c57bac8d3ba9feed989289b20)] [3] (https://android.googlesource.com/kernel/common/+f3a4b4d4a1fe2aface7de74ac257b8705b6de472)]	EoP	Critical	pKVM
CVE-2026-0031	A-443072657 Upstream kernel (https://android.googlesource.com/kernel/common/+986614312222d4b3bdcf16840cdb4abdaed8a42d)] [2] (https://android.googlesource.com/kernel/common/+aff2255dbe38dc7c57bac8d3ba9feed989289b20)] [3] (https://android.googlesource.com/kernel/common/+f3a4b4d4a1fe2aface7de74ac257b8705b6de472)]	EoP	Critical	pKVM
CVE-2025-39946	A-432728472 Upstream kernel (https://android.googlesource.com/kernel/common/+1257aa4519ee5d49e465b0dcc85cc7e4a24619d5)] [2] (https://android.googlesource.com/kernel/common/+c4bcbf924ba0823fcdc960c02e0409dbcd345a5)] [3] (https://android.googlesource.com/kernel/common/+8f4e429a1e36e588f434772dceca9068dc1208cc)	EoP	High	TLS

CVE-2025-40266	A-439862698 Upstream kernel (https://android.googlesource.com/kernel/common/+c562f4013ec6771ede259cbec802c85dfdf00e) [2 (https://android.googlesource.com/kernel/common/+a45fbd0b57716dd1cc1dd5cfcf7a2756afcbc263)] [3 (https://android.googlesource.com/kernel/common/+8cb652476b6303efe2584d38be8b20a84c141f95)]	EoP	High	pKVM
----------------	--	-----	------	------

CVE-2026-0032	A-439996285 Upstream kernel (https://android.googlesource.com/kernel/common/+048aebb861d2f3ed4d260a4c9f4e72a43cae9b1e) [2 (https://android.googlesource.com/kernel/common/+33eb6bde43d03bd826214bbb390de62ca19621b9)]	EoP	High	pKVM
---------------	---	-----	------	------

Arm components

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

CVE	References	Severity	Subcomponent
CVE-2025-2879	A-427973176_* (#asterisk)	High	Mali

Imagination Technologies

These vulnerabilities affect Imagination Technologies components and further details are available directly from Imagination Technologies. The severity assessment of these issues is provided directly by Imagination Technologies.

CVE	References	Severity	Subcomponent
CVE-2025-10865	A-449129642_* (#asterisk)	High	PowerVR-GPU
CVE-2025-13952	A-464496427_* (#asterisk)	High	PowerVR-GPU
CVE-2025-58407	A-449121737_* (#asterisk)	High	PowerVR-GPU
CVE-2025-58408	A-429381685_* (#asterisk)	High	PowerVR-GPU
CVE-2025-58409	A-440384860_* (#asterisk)	High	PowerVR-GPU
CVE-2025-58411	A-449122377_* (#asterisk)	High	PowerVR-GPU

MediaTek components

These vulnerabilities affect MediaTek components and further details are available directly from MediaTek. The severity assessment of these issues is provided directly by MediaTek.

CVE	References	Severity	Subcomponent
CVE-2025-20795	A-457250114 M-ALPS10276761_* (#asterisk)	High	KeyInstall

CVE-2026-20425	A-473379718 M-ALPS10320471_*(#asterisk)	High	display
CVE-2026-20426	A-473321948 M-ALPS10320471_*(#asterisk)	High	display
CVE-2026-20427	A-473385373 M-ALPS10320471_*(#asterisk)	High	display
CVE-2026-20428	A-473385374 M-ALPS10320471_*(#asterisk)	High	display
CVE-2026-20434	A-473385376 M-MOLY00782946_*(#asterisk)	High	Modem
CVE-2025-20760	A-457246939 M-MOLY01676750_*(#asterisk)	High	Modem
CVE-2025-20761	A-457250116 M-MOLY01311265_*(#asterisk)	High	Modem
CVE-2025-20762	A-457246938 M-MOLY01685181_*(#asterisk)	High	Modem
CVE-2025-20793	A-457250115 M-MOLY01430930_*(#asterisk)	High	Modem
CVE-2025-20794	A-457251533 M-MOLY01689259_*(#asterisk) M-MOLY01586470_*(#asterisk)	High	Modem
CVE-2026-20401	A-464955064 M-MOLY01738310_*(#asterisk)	High	Modem
CVE-2026-20402	A-464955066 M-MOLY00693083_*(#asterisk)	High	Modem
CVE-2026-20403	A-464955070 M-MOLY01689259_*(#asterisk) M-MOLY01689254_*(#asterisk)	High	Modem
CVE-2026-20404	A-464812757 M-MOLY01689248_*(#asterisk)	High	Modem
CVE-2026-20405	A-464956288 M-MOLY01688495_*(#asterisk)	High	Modem
CVE-2026-20406	A-464956289 M-MOLY01726634_*(#asterisk)	High	Modem
CVE-2026-20420	A-464812755 M-MOLY01738313_*(#asterisk)	High	Modem
CVE-2026-20421	A-464956284 M-MOLY01738293_*(#asterisk)	High	Modem

CVE-2026-20422	A-464955069 M-MOLY00827332 * (#asterisk)	High	Modem
----------------	---	------	-------

Misc OEM

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

CVE	References	Severity	Subcomponent
CVE-2025-48613	A-416491056 * (#asterisk)	High	VBMeta

Unisoc components

These vulnerabilities affect Unisoc components and further details are available directly from Unisoc. The severity assessment of these issues is provided directly by Unisoc.

CVE	References	Severity	Subcomponent
CVE-2025-61612	A-472608390 U-3145406 * (#asterisk)	High	Modem
CVE-2025-61613	A-472608389 U-3145409 * (#asterisk)	High	Modem
CVE-2025-61614	A-472596020 U-3145411 * (#asterisk)	High	Modem
CVE-2025-61615	A-472596019 U-3145413 * (#asterisk)	High	Modem
CVE-2025-61616	A-472596017 U-3145415 * (#asterisk)	High	Modem
CVE-2025-69278	A-472608387 U-3145418 * (#asterisk)	High	Modem
CVE-2025-69279	A-472596366 U-3145421 * (#asterisk)	High	Modem

Qualcomm components

These vulnerabilities affect Qualcomm components and are described in further detail in the appropriate Qualcomm security bulletin or security alert. The severity assessment of these issues is provided directly by Qualcomm.

CVE	References	Severity	Subcomponent
CVE-2025-47388	A-449733645 QC-CR#4207075 (https://git.codelinaro.org/clo/le/platform/vendor/qcom/opensource/dsp-kernel/-/commit/000ac1c2eaa3aedcdf358ed31ac03084fb553cae)	High	Security

CVE-2025-47394	A-449732573 QC-CR#4202921 (https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/dsp-kernel/-/commit/3caf9e1f6d156a7b8c5f44a60f382b1dd4b65416)	High	Kernel
CVE-2025-47396	A-449733129 QC-CR#4204623 (https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/graphics-kernel/-/commit/c2b492f15e1ab29562f2b599addcf4cc97ab90ca)	High	Display
CVE-2025-47397	A-457747735 QC-CR#4205207 (https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/graphics-kernel/-/commit/f9d053312c902b5e946491598477d0c08c6a5a24) [2] (https://git.codelinaro.org/clo/la/kernel/msm-5.10/-/commit/e797f7735703e8057c61695e2d29f3d123eab678)]	High	Display
CVE-2025-47398	A-457746802 QC-CR#4229974 (https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/graphics-kernel/-/commit/54e2054165bcd8684a985f67cadb045a1b560569) [2] (https://git.codelinaro.org/clo/la/kernel/msm-5.10/-/commit/b129548874bad5b31a3f750fb85447fd9e1d693a)]	High	Display
CVE-2025-59600	A-465462602 QC-CR#4249775 (https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/graphics-kernel/-/commit/5f90b4a23b89bbd448a0938e19357f4c67cffe9e) [2] (https://git.codelinaro.org/clo/la/kernel/msm-5.10/-/commit/9f3036379c58ebb81ab3bf1dc98dc12386a1fb3c)]	High	Display
CVE-2026-21385	A-478214401 QC-CR#4387106 (https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/graphics-kernel/-/commit/91a0db3aa438bffd235df8301bf188dbab218b7) [2] (https://git.codelinaro.org/clo/la/kernel/msm-5.4/-/commit/2a3a06da63495bf6483d9d9969b4420f4f981c50)]	High	Display

Qualcomm closed-source components

These vulnerabilities affect Qualcomm closed-source components and are described in further detail in the appropriate Qualcomm security bulletin or security alert. The severity assessment of these issues is provided directly by Qualcomm.

CVE	References	Severity	Subcomponent
CVE-2025-47339	A-430042394_* (#asterisk)	High	Closed-source component
CVE-2025-47346	A-430043562_* (#asterisk)	High	Closed-source component
CVE-2025-47348	A-430043784_* (#asterisk)	High	Closed-source component

CVE-2025-47366	A-436259280_* (#asterisk)	High	Closed-source component
CVE-2025-47378	A-442620485_* (#asterisk)	High	Closed-source component
CVE-2025-47385	A-442621008_* (#asterisk)	High	Closed-source component
CVE-2025-47395	A-449732115_* (#asterisk)	High	Closed-source component
CVE-2025-47402	A-457748468_* (#asterisk)	High	Closed-source component

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) (https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices).

- Security patch levels of 2026-03-01 or later address all issues associated with the 2026-03-01 security patch level.
- Security patch levels of 2026-03-05 or later address all issues associated with the 2026-03-05 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]:[2026-03-01]
- [ro.build.version.security_patch]:[2026-03-05]

For some devices on Android 10 or later, the Google Play system update will have a date string that matches the 2026-03-01 security patch level. Please see [this article](https://support.google.com/android/answer/7680439) (<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 2026-03-01 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 2026-03-05 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) (<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) (<https://source.android.com/security/bulletin/pixel>), [Huawei](https://consumer.huawei.com/en/support/bulletin/) (<https://consumer.huawei.com/en/support/bulletin/>), [LGE](https://lgsecurity.lge.com/security_updates_mobile.html) (https://lgsecurity.lge.com/security_updates_mobile.html), [Motorola](https://motorola-global-portal.custhelp.com/app/software-security-page/g_id/6806) (https://motorola-global-portal.custhelp.com/app/software-security-page/g_id/6806), [Nokia](https://www.nokia.com/phones/en_int/security-updates) (https://www.nokia.com/phones/en_int/security-updates), or [Samsung](https://security.samsungmobile.com/securityUpdate.smsb) (<https://security.samsungmobile.com/securityUpdate.smsb>).

Versions

Version	Date	Notes
1.0	March 2, 2026	Bulletin published
1.1	March 4, 2026	AOSP Links Added
1.2	March 9, 2026	Updated Issue List
1.3	March 10, 2026	Updated Issue List
1.4	April 2, 2026	Updated Issue List

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

Last updated 2026-04-07 UTC.