

Pixel Update Bulletin—June 2020

Published June 01, 2020 | Updated October 27, 2020

The Pixel Update Bulletin contains details of security vulnerabilities and functional improvements affecting [supported Pixel devices](https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices) (Google devices). For Google devices, security patch levels of 2020-06-05 or later address all issues in this bulletin and all issues in the June 2020 Android Security Bulletin. 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).

All supported Google devices will receive an update to the 2020-06-05 patch level. We encourage all customers to accept these updates to their devices.

Note: The Google device firmware images are available on the [Google Developer site](https://developers.google.com/android/images).

Announcements

- In addition to the security vulnerabilities described in the June 2020 Android Security Bulletin, Google devices also contain patches for the security vulnerabilities described below. When applicable, partners were notified that these issues are being addressed, and may choose to incorporate them as part of their device updates.

Security patches

Vulnerabilities are grouped under the component that they affect. There is a description of the issue and a table with the CVE, associated references, [type of vulnerability](#) (#type), [severity](#) (/docs/security/overview/updates-resources#severity), and updated Android Open Source Project (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.

Android runtime

CVE	References	Type	Severity	Updated AOSP versions
CVE-2020-0166	A-124526860	EoP	Moderate	10
CVE-2020-0187	A-148517383	ID	Moderate	10

Framework

CVE	References	Type	Severity	Updated AOSP versions
CVE-2020-0124	A-140237592 [2] https://android.googlesource.com/platform/art/+1b536ca76e1c2af297f38ece2f8b1e3e1859c9df] [3] https://android.googlesource.com/platform/frameworks/native/+331ea664c89d24657a533aeb16952a47762bbc42] [4] https://android.googlesource.com/platform/frameworks/base/+d9cb95d5c9f781357a726e1d2640563bf6c22d9d]	EoP	Moderate	10
CVE-2020-0203	A-146313311	EoP	Moderate	10
CVE-2020-0208	A-145207098	EoP	Moderate	10
CVE-2020-0209	A-145206842	EoP	Moderate	10
CVE-2020-0210	A-145206763	EoP	Moderate	10
CVE-2020-0135	A-150949837	ID	Moderate	10
CVE-2020-0167	A-129475100	ID	Moderate	10

Media framework

CVE	References	Type	Severity	Updated AOSP versions
CVE-2020-0095	A-150004253*	EoP	High	10
CVE-2020-0120	A-149995442*	EoP	High	10
CVE-2019-13135	A-136733674 (https://android.googlesource.com/platform/external/ImageMagick/+/-/2b5c0a93a867c6f46ba32ea89c1f7aef8ed44d38)	RCE	Moderate	10
CVE-2020-0131	A-151159638 (https://android.googlesource.com/platform/frameworks/av/+/-/687d14d2fe23b87c584b41b01f24e3f2596baf18)	RCE	Moderate	10
CVE-2020-0168	A-137798382 (https://android.googlesource.com/platform/external/libmpeg2/+/-/5c8de517396c1a3b5e12e6a345a8df78660cc2fc)	RCE	Moderate	10
CVE-2020-0190	A-140324890 (https://android.googlesource.com/platform/external/libmpeg2/+/-/8ff92056d7958449e31b898bdda291cc162ec87e) [2] (https://android.googlesource.com/platform/external/libmpeg2/+/-/b09e66fd455a3b8f80b36406d3f270cec9c73f1c)]	RCE	Moderate	10
CVE-2020-0194	A-143826590 (https://android.googlesource.com/platform/external/libhevc/+/-/7dcf82ada45d3dfb6e0d77a066ac619bb3a411238)	RCE	Moderate	10
CVE-2020-0126	A-137878930 (https://android.googlesource.com/platform/frameworks/av/+/-/9b7a9fcfa3051d116a19f25368ccd4a623fe72d)	EoP	Moderate	10
CVE-2020-0179	A-130656917 (https://android.googlesource.com/platform/frameworks/av/+/-/6111b2b92a1844f5796c718bf0736102b876c2b9)	EoP	Moderate	10
CVE-2020-0218	A-136005905 (https://android.googlesource.com/platform/frameworks/av/+/-/c25b042720672d0943dec638b8287ab80bedbf5d)	EoP	Moderate	10
CVE-2020-0128	A-123940919 (https://android.googlesource.com/platform/frameworks/av/+/-/2ba16f6134bd67e07ea0daa29aac5adb3155872b)	ID	Moderate	10
CVE-2019-13136	A-154008413 (https://android.googlesource.com/platform/hardware/nxp/nfc/+/-/9e2d8a17571c6a62cc6db669e51147582632bb0b) [2] (https://android.googlesource.com/platform/external/ImageMagick/+/-/2b5c0a93a867c6f46ba32ea89c1f7aef8ed44d38)]	ID	Moderate	10
CVE-2020-0127	A-140054506 (https://android.googlesource.com/platform/frameworks/opt/net/voip/+/-/0fef164d3d1f5c4e963b8142c6f9bee2ab1becc8)	ID	Moderate	10
CVE-2020-0132	A-139473816 (https://android.googlesource.com/platform/frameworks/av/+/-/b00653c6d4d06736d208a6cacfeae50e886fce49)	ID	Moderate	10
CVE-2020-0134	A-146052771 (https://android.googlesource.com/platform/frameworks/av/+/-/bb907e884ad7fee3e7c4d8fa6df45fc2402b5c4a)	ID	Moderate	10
CVE-2020-0141	A-142544793 (https://android.googlesource.com/platform/frameworks/av/+/-/75b7bf70de4093eacbd1d59738deae2d7cca4a3b)	ID	Moderate	10
CVE-2020-0151	A-133164384 (https://android.googlesource.com/platform/external/avb/+/-/ab84f1361f164e2ff20564d2d2595497ddf80ce5)	ID	Moderate	10
CVE-2020-0152	A-145992159 (https://android.googlesource.com/platform/external/avb/+/-/ab84f1361f164e2ff20564d2d2595497ddf80ce5)	ID	Moderate	10
CVE-2020-0180	A-142861738 (https://android.googlesource.com/platform/frameworks/av/+/-/6b3b2f26bbcf5ef5b41e00fc9c6bd4a164aa260)	ID	Moderate	10
CVE-2020-0182	A-147140917 (https://android.googlesource.com/platform/external/libxif/+/-/4b7b14770c4290eaaebadf0e99ffdfdb8f725c)	ID	Moderate	10
CVE-2020-0191	A-140561484 (https://android.googlesource.com/platform/external/libavc/+/-/f80afe5b98e6752ed89aef10b97863ad5db2401f)	ID	Moderate	10
CVE-2020-0192	A-144687080 (https://android.googlesource.com/platform/external/libavc/+/-/6dd54b9e180c838c8276787d10c9615af2c5866)	ID	Moderate	10
CVE-2020-0193	A-144595488 (https://android.googlesource.com/platform/external/libhevc/+/-/8d1f37478955b9d7abe5999df0511a9b9a50d95c)	ID	Moderate	10
CVE-2020-0195	A-144686961 (https://android.googlesource.com/platform/external/libhevc/+/-/fa84fd2c71b0a4cf2557ada25a38e09cb14f051)	ID	Moderate	10

CVE-2020-0197	A-137370379 (https://android.googlesource.com/platform/frameworks/av/+8e3f56b7f281a775620a9a502384cc4d87d63dfc)	ID	Moderate	10
CVE-2020-0199	A-142142406 (https://android.googlesource.com/platform/frameworks/av/+cc8271ea111a2f2119684dafa80247fd45eb4d7a)	ID	Moderate	10
CVE-2020-0200	A-147231862 (https://android.googlesource.com/platform/external/libgav1/+1ad26cf7c6a906a677ec5607e9591d4d29a4df7f) [2] (https://android.googlesource.com/platform/external/libgav1/+db2d2274ffffe028673ffd9cfea14b88d6bce68e) [3] (https://android.googlesource.com/platform/external/libgav1/+82f65a1c4a1edefdd322a58eb06c2233608c9b93) [4] (https://android.googlesource.com/platform/external/libgav1/+712c276dc8abccd5dc11b4270b213d8711d18cd2) [5] (https://android.googlesource.com/platform/external/libgav1/+ba339ef3a3f4b1b9126fa733eb23fea613b01256)	ID	Moderate	10
CVE-2020-0205	A-147234020 (https://android.googlesource.com/platform/external/libgav1/+1ad26cf7c6a906a677ec5607e9591d4d29a4df7f) [2] (https://android.googlesource.com/platform/external/libgav1/+db2d2274ffffe028673ffd9cfea14b88d6bce68e) [3] (https://android.googlesource.com/platform/external/libgav1/+82f65a1c4a1edefdd322a58eb06c2233608c9b93) [4] (https://android.googlesource.com/platform/external/libgav1/+712c276dc8abccd5dc11b4270b213d8711d18cd2) [5] (https://android.googlesource.com/platform/external/libgav1/+ba339ef3a3f4b1b9126fa733eb23fea613b01256)	ID	Moderate	10
CVE-2020-0207	A-135532289 (https://android.googlesource.com/platform/external/libyuv/+956052dd8b29293f117791e2c0d820ad5a6c55fd)	ID	Moderate	10
CVE-2020-0211	A-147491773 (https://android.googlesource.com/platform/external/libgav1/+db2d2274ffffe028673ffd9cfea14b88d6bce68e) [2] (https://android.googlesource.com/platform/external/libgav1/+1ad26cf7c6a906a677ec5607e9591d4d29a4df7f) [3] (https://android.googlesource.com/platform/external/libgav1/+82f65a1c4a1edefdd322a58eb06c2233608c9b93) [4] (https://android.googlesource.com/platform/external/libgav1/+712c276dc8abccd5dc11b4270b213d8711d18cd2)	ID	Moderate	10
CVE-2020-0212	A-135140854 (https://android.googlesource.com/platform/frameworks/av/+c155398cd771afcc93b7a7acc02946b3596a78e6)	ID	Moderate	10
CVE-2020-0160	A-124771364 (https://android.googlesource.com/platform/frameworks/av/+0db35529c7b1aaf7c08d59f22297781cf5195712)	DoS	Moderate	10
CVE-2020-0161	A-127973550 (https://android.googlesource.com/platform/frameworks/av/+ad90ca79ba8470d430032a188b6f76284f4aa9b8)	DoS	Moderate	10
CVE-2020-0162	A-124526959 (https://android.googlesource.com/platform/frameworks/av/+f562ce8410c5ffa9b28023006d20e03588e0c39d)	DoS	Moderate	10
CVE-2020-0163	A-124525515 (https://android.googlesource.com/platform/frameworks/av/+3f252fe9799ce4022db7768f63aa2d3acf7f82d6) [2] (https://android.googlesource.com/platform/frameworks/av/+6081cd380a88f04a0f2667c0f557c936645564bd)	DoS	Moderate	10
CVE-2020-0169	A-123700383 (https://android.googlesource.com/platform/cts/+7f9e1dd397495e00337b7e910bd2fa1759ce9f86) [2] (https://android.googlesource.com/platform/frameworks/av/+166a84bfe31457fe44dcb90294d33089d2a3f428)	DoS	Moderate	10
CVE-2020-0170	A-127310810 (https://android.googlesource.com/platform/cts/+7f9e1dd397495e00337b7e910bd2fa1759ce9f86) [2] (https://android.googlesource.com/platform/frameworks/av/+166a84bfe31457fe44dcb90294d33089d2a3f428)	DoS	Moderate	10
CVE-2020-0171	A-127313223 (https://android.googlesource.com/platform/cts/+7f9e1dd397495e00337b7e910bd2fa1759ce9f86) [2] (https://android.googlesource.com/platform/frameworks/av/+166a84bfe31457fe44dcb90294d33089d2a3f428)	DoS	Moderate	10
CVE-2020-0172	A-127312550 (https://android.googlesource.com/platform/cts/+7f9e1dd397495e00337b7e910bd2fa1759ce9f86) [2] (https://android.googlesource.com/platform/frameworks/av/+166a84bfe31457fe44dcb90294d33089d2a3f428)	DoS	Moderate	10
CVE-2020-0173	A-127313764 (https://android.googlesource.com/platform/cts/+7f9e1dd397495e00337b7e910bd2fa1759ce9f86) [2] (https://android.googlesource.com/platform/frameworks/av/+166a84bfe31457fe44dcb90294d33089d2a3f428)	DoS	Moderate	10
CVE-2020-0174	A-127313537 (https://android.googlesource.com/platform/cts/+7f9e1dd397495e00337b7e910bd2fa1759ce9f86) [2] (https://android.googlesource.com/platform/frameworks/av/+166a84bfe31457fe44dcb90294d33089d2a3f428)	DoS	Moderate	10
CVE-2020-0175	A-126380818 (https://android.googlesource.com/platform/frameworks/av/+166a84bfe31457fe44dcb90294d33089d2a3f428) [2] (https://android.googlesource.com/platform/external/sonivox/+40f23c8b514315113c3d790de09f63e816284538)	DoS	Moderate	10
CVE-2020-0181	A-145075076 (https://android.googlesource.com/platform/external/libexif/+f6c54954cbfc25eb73d2d2902f0597c0220174a4)	DoS	Moderate	10
CVE-2020-0184	A-141688974 (https://android.googlesource.com/platform/external/libhevc/+ae695cd67e7cd67df03ccf9afd0c014e73024fe6)	DoS	Moderate	10
CVE-2020-0189	A-139939283 (https://android.googlesource.com/platform/external/libhevc/+196e72450a1f01797c7f994d00752649407a8baa)	DoS	Moderate	10

CVE-2020-0198	A-146428941 (https://android.googlesource.com/platform/external/libexif/+1e187b62682ffab5003c702657d6d725b4278f16)	DoS	Moderate	10
---------------	--	-----	----------	----

System

CVE	References	Type	Severity	Updated AOSP versions
CVE-2020-0233	A-150225255*	EoP	High	10
CVE-2020-0138	A-142878416 (https://android.googlesource.com/platform/system/bt/+aabb0a86b51c6b962656aac19a1ab36192a27e16)	RCE	Moderate	10
CVE-2020-0217	A-141331405 (https://android.googlesource.com/platform/system/nfc/+c309b35f064c320408a32e45d12b67840a7ecc13)	RCE	Moderate	10
CVE-2020-0129	A-123292010 (https://android.googlesource.com/platform/system/bt/+7362ab9353dc09de6f0bb1c598df1139c63ae0e1)	EoP	Moderate	10
CVE-2020-0133	A-145136060 (https://android.googlesource.com/platform/packages/apps/Settings/+0d9ad30b058c165882fc098aa0c0a80cd6f6b6ec)	EoP	Moderate	10
CVE-2020-0136	A-120078455 (https://android.googlesource.com/platform/system/libhwbinder/+b022196fb65be10e5aee7bd3d5cc14ab50bb9eef) [2] (https://android.googlesource.com/platform/frameworks/native/+93fe51840ebf2e2ea0c29d3c5aa196e328129469))	EoP	Moderate	10
CVE-2020-0137	A-141920289 (https://android.googlesource.com/platform/frameworks/base/+678528ed42e98bb3e71d0efc6768ff881d04728c)	EoP	Moderate	10
CVE-2020-0150	A-142280329 (https://android.googlesource.com/platform/system/nfc/+df6cbcd43f913350125e50081e0f92b709c727b9)	EoP	Moderate	10
CVE-2020-0153	A-139733543 (https://android.googlesource.com/platform/hardware/nxp/nfc/+95ff95f8e286fc244d95bf8783410d03272c63a8)	EoP	Moderate	10
CVE-2020-0155	A-139736386 (https://android.googlesource.com/platform/hardware/nxp/nfc/+4e4e0923eb1841698ad539403b7c0687bb2920b0)	EoP	Moderate	10
CVE-2020-0165	A-139532977 (https://android.googlesource.com/platform/hardware/nxp/nfc/+9e2d8a17571c6a62cc6db669e51147582632bb0b)	EoP	Moderate	10
CVE-2020-0177	A-126206353 (https://android.googlesource.com/platform/packages/apps/Bluetooth/+5626dea3f8440ceb1d8ba75d03a57c892a6f4160)	EoP	Moderate	10
CVE-2020-0183	A-110181479 (https://android.googlesource.com/platform/system/bt/+f6275c697f7427edad7f59cf0493adfc85a2ebc0) [2] (https://android.googlesource.com/platform/packages/apps/Bluetooth/+363c6e02b9dd76f242564de31433180302bb27de)) [3 (https://android.googlesource.com/platform/frameworks/base/+d61f3f9ce1df28e7d5be040550dfe95c57a4f0a0))	EoP	Moderate	10
CVE-2020-0186	A-146144463 (https://android.googlesource.com/platform/hardware/st/nfc/+1c99651802b551f31040ec0c1232b43f89732426)	EoP	Moderate	10
CVE-2020-0188	A-147355897 (https://android.googlesource.com/platform/packages/apps/Settings/+91399607fcbcdc5fa4a26de2e7a5f175653af89c)	EoP	Moderate	10
CVE-2020-0201	A-143601727 (https://android.googlesource.com/platform/packages/apps/Settings/+f3848729b416a20a3d5d4b1a8e5a8794f727cbdc)	EoP	Moderate	10
CVE-2020-0204	A-136498130 (https://android.googlesource.com/platform/bootable/recovery/+ba27adbbb6db81babc1ee3ac070ea6b6189dd2e1)	EoP	Moderate	10
CVE-2020-0216	A-126204073 (https://android.googlesource.com/platform/packages/apps/Nfc/+8888666b6e4612e94d43c1172f6a0f9528e64a32)	EoP	Moderate	10
CVE-2020-0219	A-122836081 (https://android.googlesource.com/platform/packages/apps/Settings/+f8396c5cc0293d7231a3e73dc9b09718d25b65ed)	EoP	Moderate	10
CVE-2020-0139	A-145520471 (https://android.googlesource.com/platform/system/nfc/+ca2f591f90ddfa6c9f4d9d19d751a34e9704f13)	ID	Moderate	10
CVE-2020-0140	A-146053215 (https://android.googlesource.com/platform/system/nfc/+afd41fb6681d0d7550f8fea91e4104db05248aea)	ID	Moderate	10
CVE-2020-0142	A-146435761 (https://android.googlesource.com/platform/system/nfc/+7cd831f7b3bd1e6e6f99edcb6481f09f93f22351)	ID	Moderate	10
CVE-2020-0143	A-145597277 (https://android.googlesource.com/platform/system/nfc/+97d2416a6b2c29a55af0fd33964f5c1f643fabce)	ID	Moderate	10
CVE-2020-0144	A-142543497 (https://android.googlesource.com/platform/system/bt/+1afad0579dc76ff04c19169453e76b6617f573f5)	ID	Moderate	10

CVE-2020-0145	A-142544079 (https://android.googlesource.com/platform/system/bt/+1afad0579dc76ff04c19169453e76b6617f573f5)	ID	Moderate	10
CVE-2020-0146	A-142546561 (https://android.googlesource.com/platform/system/bt/+1afad0579dc76ff04c19169453e76b6617f573f5)	ID	Moderate	10
CVE-2020-0147	A-142638392 (https://android.googlesource.com/platform/system/bt/+1afad0579dc76ff04c19169453e76b6617f573f5)	ID	Moderate	10
CVE-2020-0148	A-142638492 (https://android.googlesource.com/platform/system/bt/+1afad0579dc76ff04c19169453e76b6617f573f5)	ID	Moderate	10
CVE-2020-0149	A-142544089 (https://android.googlesource.com/platform/system/bt/+1afad0579dc76ff04c19169453e76b6617f573f5)	ID	Moderate	10
CVE-2020-0154	A-141550919 (https://android.googlesource.com/platform/system/nfc/+3f1ae1a26e11944a4e21f369f1e1351722ca7942)	ID	Moderate	10
CVE-2020-0156	A-139736127 (https://android.googlesource.com/platform/hardware/nxp/nfc/+6ece5eb6ee400b4b263ab9409b92527f21fb063a)	ID	Moderate	10
CVE-2020-0157	A-139740814 (https://android.googlesource.com/platform/system/nfc/+c3a2dab1a0153de251fb7142dda227dab01ab12b)	ID	Moderate	10
CVE-2020-0158	A-141547128 (https://android.googlesource.com/platform/system/nfc/+0e108e626d7399f89a4bb0c4f1e782490dd2deb3)	ID	Moderate	10
CVE-2020-0159	A-140768035 (https://android.googlesource.com/platform/system/nfc/+bdb74421e9382d4aa3d0ebeb5fed81693ee64071)	ID	Moderate	10
CVE-2020-0164	A-139736125 (https://android.googlesource.com/platform/hardware/nxp/nfc/+9e2d8a17571c6a62cc6db669e51147582632bb0b)	ID	Moderate	10
CVE-2020-0176	A-79702484 (https://android.googlesource.com/platform/system/bt/+315848a18ff5c31962d70ff3ef7878b46c1f27bf)	ID	Moderate	10
CVE-2020-0178	A-143299398 (https://android.googlesource.com/platform/frameworks/base/+eb2116bd30a5c8ce2f120f3ccd341ce42009b392)	ID	Moderate	10
CVE-2020-0185	A-79945152 (https://android.googlesource.com/platform/system/bt/+9098e2a33685ba6795e7a26edf5fa89ad80f877)	ID	Moderate	10
CVE-2020-0214	A-140292264 (https://android.googlesource.com/platform/system/nfc/+320e762a3da100b9f3fa17d0ae1b4a6641bdcce8)	ID	Moderate	10
CVE-2019-16275	A-145681598 (https://android.googlesource.com/platform/external/wpa_supplicant_8/+7899587b4b28e85da84f856ee0c79b23955539d6)	DoS	Moderate	10
CVE-2020-0196	A-144066833 (https://android.googlesource.com/platform/system/bt/+90786209749a5b3523adc25769e9d15bb475f3aa)	DoS	Moderate	10
CVE-2020-0206	A-136005061 (https://android.googlesource.com/platform/packages/apps/Settings/+59f734298665ea973df7fea98bb77671100ceb54)	DoS	Moderate	10

Kernel components

CVE	References	Type	Severity	Component
CVE-2019-18683	A-145794623 Upstream kernel (https://android.googlesource.com/kernel/common/+4a2c9b037a08)	EoP	Moderate	V4L2
CVE-2019-19526	A-146258319 Upstream kernel (https://android.googlesource.com/kernel/common/+6af3aa57a098)	EoP	Moderate	NFC driver
CVE-2019-19529	A-146258054 Upstream kernel (https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4d6636498c41891d0482a914dd570343a838ad79)	EoP	Moderate	mcba USB driver
CVE-2019-19543	A-148498008 Upstream kernel (https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=56cd26b618855c9af48c8301aa6754ced8dd0beb)	EoP	Moderate	IR driver
CVE-2019-19767	A-146972026 Upstream kernel (https://github.com/torvalds/linux/commit/4ea99936a1630f51fc3a2d61a58ec4a1c4b7d55a)	EoP	Moderate	ext4
CVE-2020-0223	A-135130450* (#asterisk)	EoP	Moderate	Audio
CVE-2020-0232	A-151453714* (#asterisk)	EoP	Moderate	Airbrush

CVE-2020-0234	A-148189280* (#asterisk)	EoP	Moderate	Audio
CVE-2020-0235	A-135129430* (#asterisk)	EoP	Moderate	Audio
CVE-2020-0305	A-153467744 Upstream kernel (https://android.googlesource.com/kernel/common/+68faa679b8be1a74e6663c21c3a9d25d3)	EoP	Moderate	Kernel
CVE-2019-18786	A-148387117 Upstream kernel (https://android.googlesource.com/kernel/common/+3feec8968211)	ID	Moderate	R-Car DRIF Driver
CVE-2019-19071	A-145044845 Upstream kernel (https://github.com/torvalds/linux/commit/d563131ef23cbc756026f839a82598c8445bc45f)	DoS	Moderate	RSL91x WiFi Driver

Qualcomm components

CVE	References	Type	Severity	Component
CVE-2019-10501	A-123583662 QC-CR#2399130 (https://source.codeaurora.org/quic/la/platform/hardware/qcom/audio/commit/?id=3b7089ae44fb02dd603ec2acacc0d86e4baa5c67)	N/A	Moderate	Audio
CVE-2019-10626	A-145550580 QC-CR#2495465 (https://source.codeaurora.org/quic/la/platform/vendor/opensource/audio-kernel/commit/?id=6356fbbc1c2aa6bac2082a1f9e0ebe9efee4baff) [2 (https://source.codeaurora.org/quic/la/kernel/msm-4.4/commit/?id=88c1b337920ea92b3f620e629215fb6a4f6236c9)]	N/A	Moderate	Audio
CVE-2019-14091	A-145549566 QC-CR#2511932 (https://source.codeaurora.org/quic/la/kernel/msm-4.14/commit/?id=3c0bb7f49d2abe31e7fa30026a68dbcd4aae060)	N/A	Moderate	Kernel

Qualcomm closed-source components

CVE	References	Type	Severity	Component
CVE-2019-14092	A-145550499* (#asterisk)	N/A	Moderate	Closed-source component
CVE-2019-14094	A-145551234* (#asterisk)	N/A	Moderate	Closed-source component

Functional patches

For details on the new bug fixes and functional patches included in this release, refer to the [Pixel Community forum](https://support.google.com/pixelphone/thread/50569694) (<https://support.google.com/pixelphone/thread/50569694>).

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?

Security patch levels of 2020-06-05 or later address all issues associated with the 2020-06-05 security patch level and all previous patch levels. To learn how to check a device's security patch level, read the instructions on the [Google device update schedule](https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices) (https://support.google.com/pixelphone/answer/4457705#pixel_phones&nexus_devices).

2. 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

3. 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

4. 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 Android bug ID in the *References* column. 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>).

5. Why are security vulnerabilities split between this bulletin and the Android Security Bulletins?

Security vulnerabilities that are documented in the Android Security Bulletins are required to declare the latest security patch level on Android devices. Additional security vulnerabilities, such as those documented in this bulletin are not required for declaring a security patch level.

Versions

Version	Date	Notes
1.0	June 01, 2020	Bulletin published
1.1	June 2, 2020	Bulletin revised to include AOSP links
1.2	June 29, 2020	Revised CVE table
1.3	October 12, 2020	Entries for CVE-2020-0213 and CVE-2020-0215 updated
1.4	October 27, 2020	Revised CVE table
1.5	June 3, 2022	Revised CVE table

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 2022-08-02 UTC.