Pixel Update Bulletin—January 2021

Published January 4, 2021 | Updated January 7, 2021

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 2021-01-05 or later address all issues in this bulletin and all issues in the January 2021 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 2021-01-05 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 January 2021 Android Security Bulletin, Google devices also contain patches for the security vulnerabilities described below.

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.

Framework

CVE	References	Type	Severity	Updated AOSP versions
CVE-2020-27059	A-159249069 (https://android.googlesource.com/platform/frameworks/base/+/9588cd7de1f84a3ec8de273fb7d75921024189d8)	EoP	High	8.0, 8.1, 9, 10, 11

Kernel components

CVE	References	Type	Severity	Subcomponent
CVE-2021-0342	A-146554327 Upstream kernel (https://android.googlesource.com/kernel/common/+/96aa1b22bd6bb9fccf62f6261f390ed6f3e7967f)	EoP	Moderate	Ethernet

Qualcomm components

CVE	References	Type	Severity	Component
CVE-2020-11160	A-160613463 QC-CR#2642174 (https://source.codeaurora.org/quic/la/kernel/msm-4.14/commit/?id=622f034ee33882429424646a4a3e595b4c71baf3)	N/A	Moderate	Kernel

Qualcomm closed-source components

CVE	References	Type	Severity	Component
CVE-2020-11161	A-151169429* (#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/91975505).

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 2021-01-05 or later address all issues associated with the 2021-01-05 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).

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).

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	January 4, 2021	Bulletin published
1.1	January 7, 2021	Bulletin revised to include AOSP links

Last updated 2022-08-02 UTC.