Android Security Bulletin—January 2021

Published January 4, 2021

The Android Security Bulletin contains details of security vulnerabilities affecting Android devices. Security patch levels of 2021-01-05 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 transmission 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 January 2021 Pixel Update Bulletin.

Android and Google service mitigations

This is a summary of the mitigations provided by the Android security platform and service protections such as Google 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 and warns users about Potentially Harmful Applications. Google Play Protect is enabled by default on devices with Google Mobile Services, and is especially important for users who install apps from outside of Google Play.

2021-01-01 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2021-01-01 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, 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.

Framework

The most severe vulnerability in this section could enable a remote attacker using a specially crafted string to cause a permanent denial of service.

CVE	References	Type	Severity	Updated AOSP versions
CVE-2021-0313	A-170968514	DoS	Critical	8.0, 8.1, 9, 10, 11
CVE-2021-0303	A-170407229	EoP	High	11
CVE-2021-0306	A-154505240	EoP	High	8.0, 8.1, 9, 10, 11
CVE-2021-0307	A-155648771	EoP	High	10, 11
CVE-2021-0310	A-170212632	EoP	High	11
CVE-2021-0315	A-169763814	EoP	High	8.0, 8.1, 9, 10, 11
CVE-2021-0317	A-168319670	EoP	High	8.0, 8.1, 9, 10, 11
CVE-2021-0318	A-168211968	EoP	High	8.1, 9, 10, 11
CVE-2021-0319	A-167244818	EoP	High	8.0, 8.1, 9, 10, 11
CVE-2021-0304	A-162738636	ID	High	8.0, 8.1, 9, 10
CVE-2021-0309	A-158480899	ID	High	8.0, 8.1, 9, 10, 11
CVE-2021-0321	A-166667403	ID	High	11
CVE-2021-0322	A-159145361	ID	High	9, 10, 11
CVE-2019-9376	A-129287265	DoS	High	8.0, 8.1, 9
CVE-2020-15999	A-171232105	RCE	Moderate	8.0, 8.1, 9, 10, 11

Media Framework

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

CVE	References	Type	Severity	Updated AOSP versions
CVE-2016-6328	A-162602132	RCE	High	8.0, 8.1, 9, 10, 11
CVE-2021-0311	A-170240631	ID	High	8.0, 8.1, 9, 10, 11
CVE-2021-0312	A-170583712	ID	High	8.0, 8.1, 9, 10, 11

System

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

CVE	References	Type	Severity	Updated AOSP versions
CVE-2021-0316	A-168802990	RCE	Critical	8.0, 8.1, 9, 10, 11
CVE-2020-0471	A-169327567	EoP	High	8.0, 8.1, 9, 10, 11
CVE-2021-0308	A-158063095	EoP	High	8.0, 8.1, 9, 10, 11
CVE-2021-0320	A-169933423	ID	High	10, 11

Google Play system updates

The following issues are included in Project Mainline components.

Component	CVE
Media Framework components	CVE-2021-0311, CVE-2021-0312

2021-01-05 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2021-01-05 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.

Kernel components

The most severe vulnerability in this section could enable a local malicious application to bypass operating system protections that isolate application data from other applications.

CVE	References	Type	Severity	Component
CVE-2020-10732	A-170658976 Upstream kernel	ID	High	ELF core dumps
CVE-2020-10766	A-169505740 Upstream kernel	ID	High	Speculative execution
CVE-2021-0323	A-156766097 Upstream kernel	ID	High	Linux kernel

MediaTek components

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

CVE	References	Severity	Component
CVE-2021-0301	A-172514667 M-ALPS05342361*	High	ged

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	Component
CVE-2020-11233	A-170138863 QC-CR#2257789	High	Kernel

CVE-2020-11239	A-168722551 QC-CR#2744826	High	Display
CVE-2020-11240	A-170138526 QC-CR#2702760 [2] [3]	High	Camera
CVE-2020-11250	A-170139097 QC-CR#2734543	High	Audio
CVE-2020-11261	A-161373974 QC-CR#2742124	High	Display
CVE-2020-11262	A-170138789 QC-CR#2742711	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	Component
CVE-2020-11134	A-170138862*	Critical	Closed-source component
CVE-2020-11182	A-168722721*	Critical	Closed-source component
CVE-2020-11126	A-170139227*	High	Closed-source component
CVE-2020-11159	A-170138666*	High	Closed-source component
CVE-2020-11181	A-168051034*	High	Closed-source component
CVE-2020-11235	A-170138866*	High	Closed-source component
CVE-2020-11238	A-170139099*	High	Closed-source component
CVE-2020-11241	A-170139229*	High	Closed-source component
CVE-2020-11260	A-168918332*	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.

- Security patch levels of 2021-01-01 or later address all issues associated with the 2021-01-01 security patch level.
- 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.

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

- [ro.build.version.security_patch]:[2021-01-01]
- [ro.build.version.security_patch]:[2021-01-05]

For some devices on Android 10 or later, the Google Play system update will have a date string that matches the 2021-01-01 security patch level. Please see this article 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 2021-01-01 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 2021-01-05 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

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	January 4, 2021	Bulletin released