Android Security Bulletin November 2024

12-16 minutes

Published November 4, 2024

The Android Security Bulletin contains details of security vulnerabilities affecting Android devices. Security patch levels of 2024-11-05 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 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 high security vulnerability in the System component that could lead to remote code execution with no additional execution privileges needed. 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.

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.

2024-11-01 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2024-11-01 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 lead to local escalation of privilege with no additional execution privileges needed.

CVE	References	Type	Severity	Updated AOSP versions
CVE-2024-40660	A-347307756 [2]	EoP	High	14, 15
CVE-2024-43081	A-341256043	EoP	High	12, 12L, 13, 14, 15
CVE-2024-43085	A-353712853	EoP	High	12, 12L, 13, 14, 15
CVE-2024-43093	A-341680936	EoP	High	12, 13, 14, 15
CVE-2024-43082	A-296915959	ID	High	12, 12L
CVE-2024-43084	A-281044385	ID	High	12, 12L, 13, 14, 15
CVE-2024-43086	A-343440463	ID	High	12, 12L, 13, 14, 15

System

The most severe vulnerability in this section could lead to remote code execution with no additional execution privileges needed.

CVE	References	Type	Severity	Updated AOSP versions
CVE-2024-43091	A-344620577	RCE	High	12, 12L, 13, 14, 15
CVE-2024-29779	A-329701910	EoP	High	14
CVE-2024-34719	A-242996380	EoP	High	12, 12L, 13, 14
CVE-2024-40661	A-308138085	EoP	High	12, 12L, 13, 14
CVE-2024-43080	A-330722900	EoP	High	12, 12L, 13, 14, 15
CVE-2024-43087	A-353700779	EoP	High	12, 12L, 13, 14, 15
CVE-2024-43088	A-326057017	EoP	High	12, 12L, 13, 14, 15
CVE-2024-43089	A-304280682	EoP	High	12, 12L, 13, 14, 15

CVE-2024-43090	A-331180422	ID	High	12, 12L, 13, 14
CVE-2024-43083	A-348352288	DoS	High	12, 12L, 13, 14, 15

Google Play system updates

The following issues are included in Project Mainline components.

Subcomponent	CVE
Documents UI	CVE-2024-43093
MediaProvider	CVE-2024-43089
Permission Controller	CVE-2024-40661
WiFi	CVE-2024-43083

2024-11-05 security patch level vulnerability details

In the sections below, we provide details for each of the security vulnerabilities that apply to the 2024-11-05 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

The most severe vulnerability in this section could lead to local escalation of privilege with no additional execution privileges needed.

Kernel LTS

The following kernel versions have been updated. Kernel version updates are dependent on the version of Android OS at the time of device launch.

References	Android Launch Version	Kernel Launch Version	Minimum Update Version
A-348473863	12	5.4	5.4.274
A-348681334	12	4.19	4.19.312

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-2024-34747	A-346643520 *	High	PowerVR-GPU
CVE-2024-40671	A-355477536 *	High	PowerVR-GPU

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-2023-35659	A-350006107 *	High	PowerVR-GPU
CVE-2023-35686	A-350527097 *	High	PowerVR-GPU
CVE-2024-23715	A-350530745 *	High	PowerVR-GPU
CVE-2024-31337	A-337944529 *	High	PowerVR-GPU
CVE-2024-34729	A-331437862 *	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-2024-20104	A-363850556 M-ALPS09073261 *	High	DA
CVE-2024-20106	A-363849996 M-ALPS08960505 *	High	m4u

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.

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-2024-38408	A-357615875 *	Critical	Closed-source component
CVE-2024-23385	A-339043003 *	High	Closed-source component
CVE-2024-38403	A-357615948 *	High	Closed-source component
CVE-2024-38424	A-357616230 *	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 2024-11-01 or later address all issues associated with the 2024-11-01 security patch level.
- Security patch levels of 2024-11-05 or later address all issues associated with the 2024-11-05 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]:[2024-11-01]
- [ro.build.version.security_patch]:[2024-11-05]

For some devices on Android 10 or later, the Google Play system update will have a date string that matches the 2024-11-01 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 2024-11-01 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 2024-11-05 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.

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	November 4, 2024	Bulletin Published.