

[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)

> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)

> **Android November patch fixes actively exploited kernel bug**

Android November patch fixes actively exploited kernel bug

By

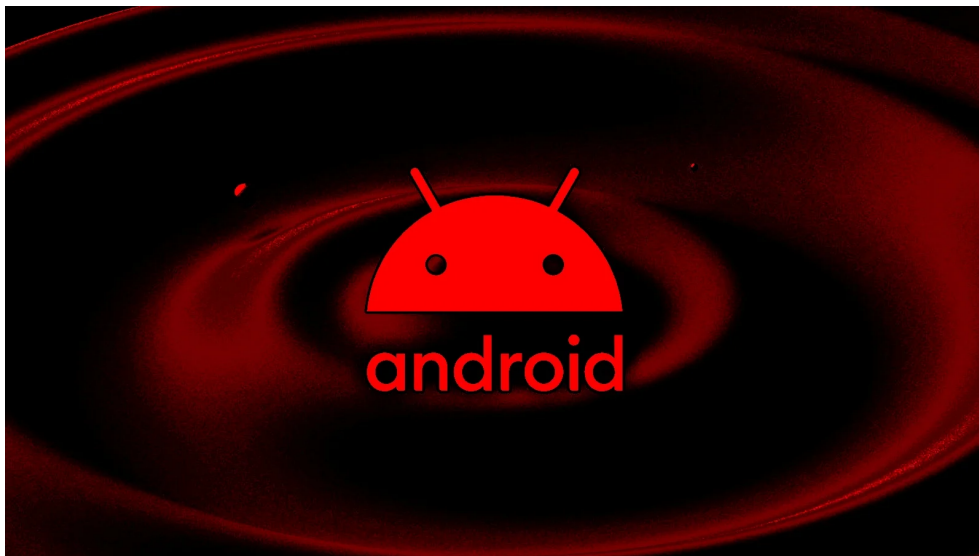
Bill Toulas

(<https://www.bleepingcomputer.com/author/bill-toulas/>)

November 2, 2021

07:01 AM

1



Google has released the Android November 2021 security updates, which address 18 vulnerabilities in the framework and system components, and 18 more flaws in the kernel and vendor components.



[Ad was inappropriate](#)[Not interested in this ad](#)[Seen this ad multiple times](#)

Not many technical details have been released around this flaw yet, as original equipment manufacturers (OEMs) are currently working on merging the patch with their custom builds, so most Android users are vulnerable.

Five critical issues

The most severe issues addressed by the November 2021 patch (<https://source.android.com/security/bulletin/2021-11-01>) are two critical System remote code execution (RCE) bugs tracked as CVE-2021-0918 and CVE-2021-0930.

These flaws enable attackers to execute arbitrary code within the context of a privileged process by sending a specially crafted transmission to the target device.

Two more critical flaw security flaws addressed with this month's patch are those for CVE-2021-1924 and CVE-2021-1975, both impacting Qualcomm components.

The fifth critical flaw fix lies in Android TV's "remote service" component and is an RCE tracked as CVE-2021-0889.

Exploiting this flaw would enable an attacker near the device to execute code without privileges or user interaction.

How Android patch levels work

As a reminder on how Android patch levels work, Google releases at least two of them each month, and for November, it's 2021-11-01, 2021-11-05, and 2021-11-06.

Those who see an update alert marked as 2021-11-01, it means that they will get the following:

- November framework patches
- October framework patches
- October vendor and kernel

Those who see either 2021-11-05 or 2021-11-06 patch levels will receive all of the above, plus the November vendor and kernel patches.



[Ad was inappropriate](#)[Not interested in this ad](#)[Seen this ad multiple times](#)

This is the first security patch for the recently-released Android 12, but many of the fixes go back to versions 11, 10, and 9, depending on the scope of the addressed vulnerabilities.

If you are using older Android versions, you are not covered by this patch level, and your device is vulnerable to yet one more actively exploited flaw.

Finally, this is the first patch level not delivered to Pixel 3, which marks the official end of support for one of Google's most beloved devices.

Related Articles:

Android October patch fixes three critical bugs, 41 flaws in total
(<https://www.bleepingcomputer.com/news/security/android-october-patch-fixes-three-critical-bugs-41-flaws-in-total/>)

Emergency Google Chrome update fixes zero-days used in attacks
(<https://www.bleepingcomputer.com/news/google/emergency-google-chrome-update-fixes-zero-days-used-in-attacks/>)

Millions of Android users targeted in subscription fraud campaign
(<https://www.bleepingcomputer.com/news/security/millions-of-android-users-targeted-in-subscription-fraud-campaign/>)

Google cuts Play Store dev fees to 15% for all subscriptions
(<https://www.bleepingcomputer.com/news/google/google-cuts-play-store-dev-fees-to-15-percent-for-all-subscriptions/>)

Study reveals Android phones constantly snoop on their users
(<https://www.bleepingcomputer.com/news/security/study-reveals-android-phones-constantly-snoop-on-their-users/>)

