Google fixes remote escalation of privileges bug on Android

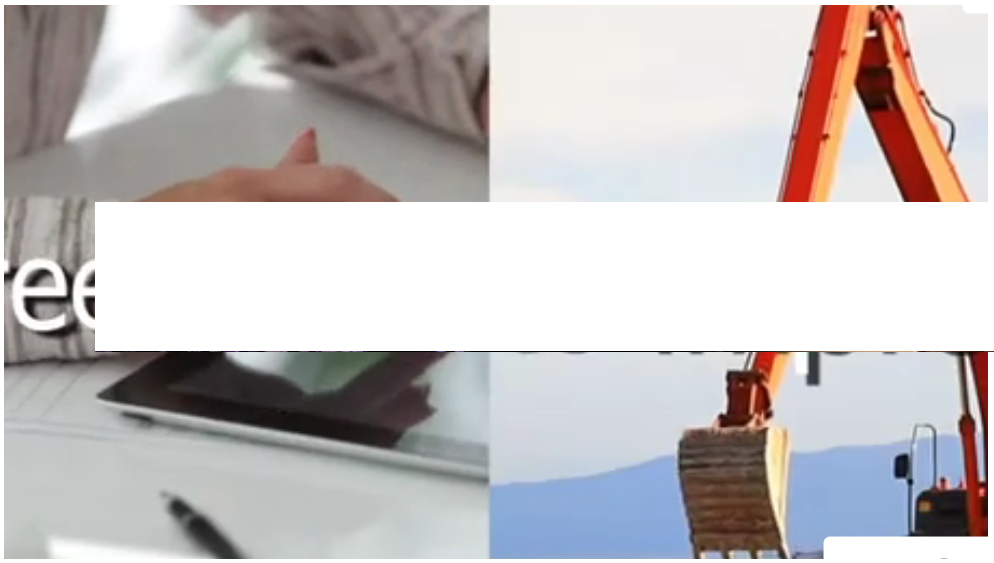
By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

February 8, 2022 04:25 PM **0**

Google has released the February 2022 Android security updates, addressing two critical vulnerabilities, one being a remote escalation of ege that requires no user interaction.

The vulnerability is tracked as CVE-2021-39675 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39675), carrying a “critical” severity rating, and affects only Android 12, the latest version of the popular OS.

These flaws are typically leveraged by sophisticated spyware vendors that independently discover and privately use zero-days in mobile operating systems. However, in this case, Google hasn’t seen any signs of active exploitation.



The second critical flaw addressed by the February 2022 security update is CVE-2021-30317 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30317), which affects a closed-source component of Qualcomm, and thus only concerns Android devices that use that vendor’s hardware.

Here’s a summary of this month’s fixes:

- Five high-severity flaws in Framework
- Four high-severity bugs in Media Framework
- Seven high-severity to critical flaws in System
- Two vulnerabilities of undefined severity in Media Provider
- One high-severity flaw in Amlogic components
- Five high-severity bugs in MediaTek components
- Three high-severity flaws in Unisoc components
- Six high to critical-severity vulnerabilities in Qualcomm components

As Google clarifies in the bulletin (http://source.android.com/security/bulletin/2022-02-01): "The severity assessment is based on the effect that exploiting the vulnerability would

The technical details about the vulnerabilities are not available at this time, as Android updates typically need several months to reach a respectable percentage of the userbase, given that vendors need to bundle them separately for each device model.

The only exception to this practice is Google's own Pixel devices, with all models from '3a' up to '6 Pro' already receiving the February 2022 security update in a simultaneous roll-out.

Finally, the fixes that come with this month's update concern Android 10, 11, and 12, so if your phone runs anything older than that, you are no longer covered, and you should consider your device a security liability.

If you don't want to replace a perfectly working electronic device that is no longer supported by its manufacturer, you could flash it with a third-party Android ROM that's based on a more recent and secure AOSP version, like Lineag

Relat

Android users can now disable 2G to block Stingray attacks (https://www.bleepingcomputer.com/news/security/android-users-can-now-disable-2g-to-block-stingray-attacks/)

Microsoft February 2022 Patch Tuesday fixes 48 flaws, 1 zero-day (https://www.bleepingcomputer.com/news/microsoft/microsoft-february-2022-patch-tuesday-fixes-48-flaws-1-zero-day/)

Microsoft January 2022 Patch Tuesday fixes 6 zero-days, 97 flaws (https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2022-patch-tuesday-fixes-6-zero-days-97-flaws/)

Apple fixes new zero-day exploited to hack macOS, iOS devices (https://www.bleepingcomputer.com/news/apple/apple-fixes-new-zero-day-exploited-to-hack-macos-ios-devices/)

Microsoft December 2021 Patch Tuesday fixes 6 zero-days, 67 flaws (https://www.bleepingcomputer.com/news/microsoft/microsoft-december-2021-patch-tuesday-fixes-6-zero-days-67-flaws/)