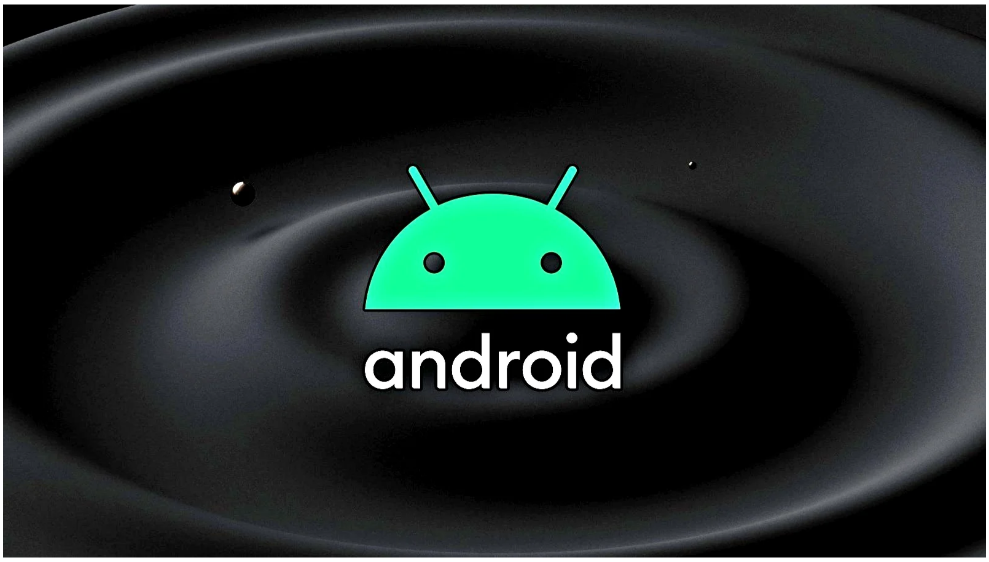
Android's March 2022 security updates fix three critical bugs

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

March 8, 2022 04:35 PM 1



Google has released the March 2022 security updates for Android 10, 11, and 12, addressing three critical severity flaws, one of which affects all devices running the latest version of the mobile OS.

Tracked as CVE-2021-39708, the flaw lies in the Android System component, and it's an escalation of privilege problem requiring no user interaction or additional execution privileges.

"The most severe of these issues is a critical security vulnerability in the System component that could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation." - mentions Google's bulletin (https://source.android.com/security/bulletin/2022-03-01).

(https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2022-patch-tuesday-fixes-71-flaws-3-zero-days/?traffic_source=Connatix)

Microsoft March 2022 Patch Tuesday fixes 71 flaws, 3 zero-days

The other two critical flaws are CVE-2021-1942 and CVE-2021-35110, both affecting closed-source components on Qualcomm-based devices.

For a full list of which Qualcomm chipsets are affected by these two vulnerabilities, check out the chipmaker's security bulletin (https://www.qualcomm.com/company/product-security/bulletins/march-2022-bulletin).

No further technical details have been published for any of the fixed vulnerabilities, as doing so would put users running an older patch level at risk.

Other fixes that land with the March 2022 update are:

- 1 medium severity escalation of privilege flaw in Android runtime (version 12)
- 5 high severity escalation of privileges flaws in Android Framework (versions 10, 11, 12)
- 2 high severity denial of service flaws in Android Framework (version 12)
- 1 high severity information disclosure in Media Framework (versions 10, 11, 12)

- 8 high severity escalation of privilege flaws in System (versions 10, 11, 12)
- 1 high severity information disclosure flaw in System (versions 10, 11, 12)
- 4 high severity escalation of privilege flaws in Kernel
- 1 high severity information disclosure in Kernel
- 3 high severity flaws in MediaTek components
- 10 high severity flaws in Qualcomm components

As is the case every month, Google has released two patch levels for March 2022, one denoted as "2022-03-01" and one as "2022-03-05".

The second patch level includes everything in the first set plus fixes for third-party closed source and Kernel components that may not apply to all devices.

As such, your device vendor may choose to push the first level to save on roll-out time, and it won't necessarily mean that you are left vulnerable to exploitation.

With the only exception being Google's Pixel line which receives these security updates immediately, all other vendors (https://security.samsungmobile.com/securityUpdate.smsb) will need some time to bundle the patches for each of their models, as different hardware configurations require dedicated testing and fine-tuning.

If you are running anything older than Android 10, consider upgrading to a new and actively supported device or flashing your existing with a third-party Android ROM that's based on a recent AOSP version.