Google warns of a vulnerability that allows Android smartphones to be attacked with just a phone number

Google researchers have discovered and reported 18 zero-day vulnerabilities in Samsung-made Exynos modems found in dozens of Android phones, watches, and vehicles.

In which, there are 4 particularly serious vulnerabilities, which can compromise the device 'remotely and quietly' with just the victim's phone number without their interaction.

These vulnerabilities have the ability to remotely run code at the baseband level of the device, allowing hackers to access data in and out of the device with almost no obstruction. Attackers can access data including cell phone calls, text messages, and mobile data.

Google further warned that experienced attackers without a lot of resources can quickly exploit the vulnerability.

Project Zero expert Maddie Stone said that Samsung had 90 days to patch the vulnerability, but the company was unable to complete it.

Samsung has also confirmed that some Exynos modems have vulnerabilities that affect several Android device manufacturers, but did not provide details.

According to Project Zero, there are nearly 12 models of Samsung, Vivo, Google Pixel 6 and Pixel 7 affected devices including Samsung S22, M33, M13, M12, A71, A53, A33, A21s, A13, A12 and A04; Vivo S16, S15, S6, X70, X60 and X30; Google Pixel 6, Pixel 7; Vehicles using Exynos Auto T5123 chip.

Patches for each device family will be rolled out depending on the manufacturer. Recently, Google rolled out a patch for Pixel phones in the March security update.

To eliminate the risk of exploiting the vulnerability, Google recommends that users protect themselves by turning off Wi-Fi and VoLTE calling on their devices, before the vendors release patches.