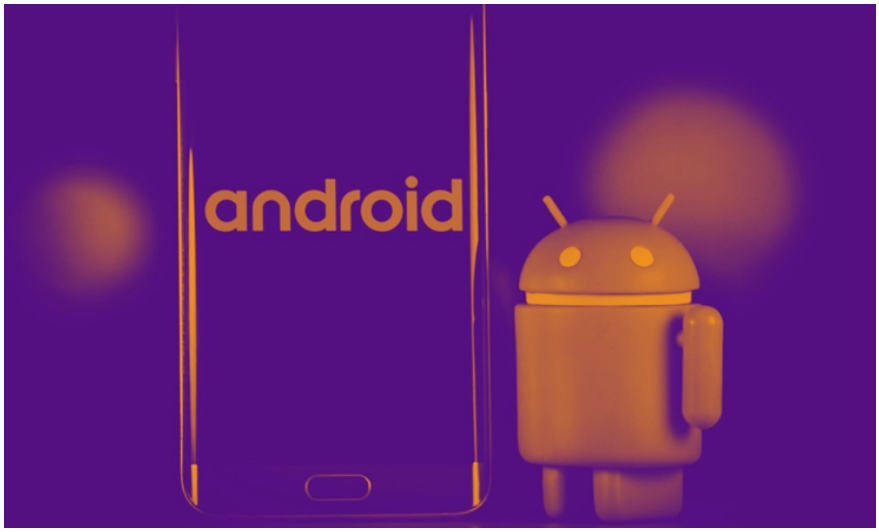
Google quietly patches USB vulnerability, billions of Android devices narrowly escape!

Google has quietly released a security patch for a serious vulnerability in its Android operating system that could put more than 1 billion devices at risk.

This vulnerability is related to USB connectivity, and was discovered and reported by Amnesty International.

The vulnerability, identified as CVE-2024-53104, is a zero-day vulnerability at the kernel level that allows an attacker to bypass the lock screen and gain deep access to the system via a USB connection. This means that hackers can steal data, install malware, or take complete control of the device.



Billions of Android devices have just escaped the risk because Google patched the vulnerability.

According to information from Amnesty International, this vulnerability was exploited in an incident involving a Serbian student activist, whose phone was illegally accessed using the Cellebrite tool.

Amnesty International has warned about the potential risks of untrusted USB connections and called on Android manufacturers to strengthen security measures.

Google also recommends that Android users update their operating system to the latest version as soon as possible to patch this vulnerability.

The case also raises ethical concerns about Cellebrite, a company that provides forensic analysis tools to law enforcement. The company claims to be able to unlock any Android or Apple device, but the use of these tools

also poses the risk of abuse for surveillance and privacy.