Global telecom gear companies cold to sharing source codes

SURAJEET DAS GUPTA
New Delhi, 27 March

Global telecom equipment manufacturers have opposed submitting the "source code" of their software as a prerequisite for selling in India, even after the government has extended the deadline until December 31, sources said.

A top European Union delegation, which recently visited India for free-trade agreement (FTA) talks, raised concerns on the contentious issue with the government.

The Communication Security Certification Scheme, notified in 2020, mandated telecom gear makers to submit their software source code to third-party test labs earmarked by the Indian government. Currently, this applies to WiFi equipment, routers, and customer premises equipment and will also include radios in the second half of this year.

European telecom companies, the hardest hit by this requirement, argue that no such mandate or practice exists globally and that source code disclosures may set an international precedent, which could compromise global intellectual property rights (IPR). They fear that centralising critical infrastructure source code could increase the risks of cyberattacks and fall into the hands of competitors. Turn to Page 6

THE CLAIMS

- Deadline for telecom gear's source code submission extended to Dec 31, 2025
- EU concerned about norm's requirements
- Global players say sharing source code could compromise their Intellectual Property Rights
- Claim no such requirements exist globally, India is not an exception

Demand for access to 'source code' not new in India

Amid growing opposition to this issue, the National Centre for Communication Security (NCCS) in October 2024 granted a temporary reprieve, relaxing the requirement for telecom gear makers to submit source code and instead allowing an internal test report. However, in February 2025, the government notified that this relaxation would only remain in place until December 31. Currently, companies can sell their products only after providing an undertaking that they will adhere to the source code rule by year-end.

Global telecom gear companies argue that their equipment already undergoes elaborate audits to ensure adherence to global security processes, including the GSMA-led, industry-funded Network Equipment Security Assurance Scheme (NESAS), which is a third-party auditor certification for telecom gear software. NESAS works with internationally recognised partners and labs that audit and test equipment under the GSMA NESAS Oversight Board. It has testing facilities across the globe. In India, companies conduct lab tests in government-accredited facilities to ensure all security protocols are met so that their clients are assured. However, what they oppose is the additional requirement to provide not only the "source code" but also their "internal reports". The demand for access to the "source code" is not new in India. In 2012, Chinese vendors Huawei and ZTE publicly offered the government unrestricted access to their software source code on all products. This was in response to the Indian government examining a report by a US Congress panel that alleged the two Chinese tech majors had direct connections with the Chinese government and military.

In 2018, Huawei again offered access to the source code and proposed keeping it in an escrow account. However, the government ultimately took a decision that prevented both Huawei and ZTE from selling their 5G gear to Indian telecom operators, effectively shutting them out of the market.