BARTEC

Document ID	Title	Version	Date
11-S190-6B0019	Android Network Interfaces and Exposed Services – Security Notice	1.0	2025-10-10

Author	Document Responsible	Approved By
Fredrik Öijer	Fredrik Öijer	Sebastian Kuhn

Android Network Interfaces and Exposed Services – Security Notice

This document informs the user that the following network interfaces and services exist on the device and may pose potential security vulnerabilities if misconfigured or exploited.

Network Interface / Service	Description	Potential Vulnerability Risk
Wi-Fi (802.11 a/b/g/n/ac/ax)	Wireless local-area connection to access points and networks.	Exposure to untrusted networks, man-in-the-middle (MitM) attacks, spoofed access points, or weak WPA configuration.
Cellular (4G / 5G)	Mobile data connectivity via carrier infrastructure.	Possible interception or tracking through rogue base stations or insecure carrier provisioning.
USB-C (Tethering / ADB)	Physical interface for charging, data transfer, and debugging.	Risk of data exfiltration or unauthorized access when USB debugging (ADB) or tethering is enabled.
Bluetooth	Short-range wireless connectivity for peripherals.	Susceptible to unauthorized pairing, data leakage, or proximity attacks if left discoverable.
NFC	Near-Field Communication for tap-based data exchange or payments.	Risk of unintended data exchange or malicious NFC tags if NFC is enabled in public spaces.
Ethernet via USB-C Dongle	Wired network interface for direct LAN access.	Exposure to untrusted LANs; possible MitM or ARP-spoofing attacks.

Wi-Fi Hotspot / Tethering	Shares device's data connection with other clients.	Unauthorized client connections or data misuse if hotspot credentials are weak or shared publicly.
Android System Update Service	Connects to Google / OEM servers to download system updates.	Potential risk if update channels are intercepted or spoofed on untrusted networks.
EMM / MDM Agent Communication	Communicates with enterprise management servers.	May expose device identifiers or config data if misconfigured; depends on enterprise policy.
Push Notification (Google FCM)	Receives background messages and notifications.	Risk of information leakage or app-level abuse if apps misuse push channels.
Google Play Services (incl. FCM)	Core background framework for Google APIs and updates.	Network activity may reveal metadata; ensure Play Protect and verified apps are enabled.
Location Services (Network-Assisted)	Uses Wi-Fi and cellular data to assist GPS location.	Potential location tracking or privacy leakage if location permissions are mismanaged.

User Guidance

- Keep Wi-Fi, Bluetooth, and NFC off when not in use.
- Enable USB debugging only when needed.
- Use strong hotspot passwords and trusted networks.
- Install system updates only through official channels.
- Review app permissions regularly, especially for network and location access.