SPC-13 · Mobile Threat Catalogue

Archived: 2026-04-06 03:25:58 UTC

Mobile Threat Catalogue

Hardware Design and Manufacture Compromise

Contribute

Threat Category: Supply Chain

ID: SPC-13

Threat Description: The design and manufacture of critical hardware at targeted suppliers can be compromised.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Employ software integrity verification checks on firmware, which can be validated against a known-good value (e.g. brute-force resistant cryptographic hash of firmware image) to detect any modification

Obtain device measurements for comparison to normal ranges (e.g., temperature, timing, EM radiation, power consumption) to detect anomalous behavior in received components prior to production use.

References

1. J.F. Miller, “Supply Chain Attack Framework and Attack Patterns”, tech. report, MITRE, Dec. 2013; www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf ↩ ↩[2]
