SPC-1 · Mobile Threat Catalogue

Archived: 2026-04-05 18:20:39 UTC

Mobile Threat Catalogue

Hardware or Firmware Component Interception

Contribute

Threat Category: Supply Chain

ID: SPC-1

Threat Description: A hardware or firmware component can be intercepted by an adversary while in transit between supplier and acquirer, for the purpose of substitution or manipulation.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

CVE Examples

Possible Countermeasures

Enterprise

Require firmware to be digitally signed by a trusted developer and the signature verified prior to the component being integrated into a larger system

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

Obtain device measurements for comparison to normal ranges (e.g., temperature, timing, EM radiation, power consumption) to detect anomalous behavior.

References
