# SPC-8 · Mobile Threat Catalogue

Archived: 2026-04-05 23:19:16 UTC

## Mobile Threat Catalogue

## Firmware Component Substitution During Transfer

Contribute

**Threat Category:** Supply Chain

**ID:** SPC-8

**Threat Description:** An adversary with access to supplier shipping channels during transfer of system components can substitute a counterfeit firmware component for an authentic component.[1]

**Threat Origin**

Supply Chain Attack Framework and Attack Patterns [1]

**Exploit Examples**

*Not Applicable*

**CVE Examples**

*Not Applicable*

**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**

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]

Source: https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-8.html