SPC-6 · Mobile Threat Catalogue

Archived: 2026-04-06 01:54:13 UTC

Mobile Threat Catalogue

Improperly Vetted or Untested Malicious Microelectronics

Contribute

Threat Category: Supply Chain

ID: SPC-6

Threat Description: An adversary with access to the hardware commodity procurement process can insert improperly vetted or untested malicious critical microelectronics components into the system during development.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Require that hardware components be tested for correct functionality and normal operation, and that the output of automated testing processes be digitally signed by the component that performed the test, and that the results are verified prior to acceptance of the tested component into the next stage of procurement, development, or deployment to reduce the likelihood an adversary can successfully introduce a malicious component that is not detected prior to use in production

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-6.html