SPC-2 · Mobile Threat Catalogue

Archived: 2026-04-06 03:11:02 UTC

Mobile Threat Catalogue

Malicious Critical Hardware Replacement

Contribute

Threat Category: Supply Chain

ID: SPC-2

Threat Description: Adversarial supply chain distribution channel personnel (e.g., packaging, shipping, receiving, or transfer) can intercept and replace legitimate critical hardware components with malicious ones.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Perform background checks on supply chain personnel as appropriate to the level of sensitivity of the component being distributed to detect placement or the potential for or actual manipulation by an adversary

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]
