

# SPC-5 · Mobile Threat Catalogue

Archived: 2026-04-06 01:56:56 UTC

## [Mobile Threat Catalogue](#)

### Malware Embedded in Critical Component

#### [Contribute](#)

**Threat Category:** Supply Chain

**ID:** SPC-5

**Threat Description:** An adversary with access to hardware procurement, maintenance, or upgrade control can embed malware in a critical component.<sup>1</sup>

#### Threat Origin

Supply Chain Attack Framework and Attack Patterns <sup>1</sup>

#### Exploit Examples

*Not Applicable*

#### CVE Examples

*Not Applicable*

#### Possible Countermeasures

##### Enterprise

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

Test hardware to verify it functions as expected (e.g. known inputs yield correct outputs) prior to placing or replacing the device into the production environment

#### 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](http://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf) [↔](#) [↔](#)<sup>2</sup>