SPC-4 · Mobile Threat Catalogue

Archived: 2026-04-05 21:23:36 UTC

Mobile Threat Catalogue

Malicious Logic Introduction

Contribute

Threat Category: Supply Chain

ID: SPC-4

Threat Description: A software or firmware programmer with access to the configuration control system can introduce malicious logic into software or microelectronics during coding and/or logic-bearing component development or update/maintenance.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Enforce strict access control and auditing for the configuration control system to enable effective auditing of any unauthorized changes to configuration settings.

Use configuration management tools that can validate that current configuration settings meet policy requirements

Test software and microelectronics to verify their functionality conforms to expected behavior and operates within normal tolerances (e.g. timing, temperature, power consumption, EM emissions) both after development and maintenance prior to placing or returning the component to 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 ↩ ↩2
