SPC-9 · Mobile Threat Catalogue

Archived: 2026-04-06 01:28:58 UTC

Mobile Threat Catalogue

Malicious Code in Custom Software

Contribute

Threat Category: Supply Chain

ID: SPC-9

Threat Description: An adversary with access privileges within the software development environment and to associated tools, including the software unit/component test system and the software configuration management system, can hide malicious code in custom software.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Require test results to be digitally signed by both the testing component and a credential uniquely associated with the test operator to enforce non-repudiation

Enforce strict access control and auditing for software testing systems to enable effective auditing of tests

Design testing processes such that individuals responsible for testing do not know the destination of a tested component to prevent sabotage of a specific critical function, location, device, or organizational operation

Design testing processes that use at least two independent testers/processes/tools and compare test results for consistency

For mission-critical components, randomly test the same component multiple times using different testers/processes/tools and compare test results for consistency

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
