SPC-10 · Mobile Threat Catalogue

Archived: 2026-04-05 20:45:19 UTC

Mobile Threat Catalogue

Malicious Software in 3rd Party Bundling Process

Contribute

Threat Category: Supply Chain

ID: SPC-10

Threat Description: An adversary with access to 3rd party bundling processes and tools can implant malicious software in a system during the hardware-software integration phase.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Test systems that contain newly integrated or updated software components to detect incorrect function or anomalous behavior prior to production use

Obtain direct from the software developer a list of files changed by the installation or upgrade process, and if possible, strong cryptographic hashes for file updates that are configuration-independent and should produce known values

Use fine-grained role-based access control mechanisms and user/service roles that reduce the potential that malicious installation or upgrade packages can introduce malware outside of files and directories allocated to the associated software

Scan systems with newly integrated or updated software components for indicators of compromise prior to production use

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]
