SPC-3 · Mobile Threat Catalogue

Archived: 2026-04-05 12:41:44 UTC

Mobile Threat Catalogue

Contribute

Threat Category: Supply Chain

ID: SPC-3

Threat Description: An adversary with access to software processes and tools within the development or software support environment can insert malicious software into components during development or update/maintenance.[1]

Threat Origin

Supply Chain Attack Framework and Attack Patterns [1]

Symantec Internet Security Threat Report 2016 [2]

Exploit Examples

XcodeGhost distributed a malicious version of Xcode (Apple''s developer tools) that automatically includes malicious code in compiled iOS apps.

CVE Examples

Possible Countermeasures

Mobile App Developer

App developers should ensure that development tools are obtained from a trusted source (e.g. directly from the vendor).

Enterprise

Only software digitally signed by a trusted developer should be used, and the integrity of software development installation packages should be verified prior to installation

Obtained software should be installed onto target operating systems in a known-good state (fresh install from verified installation media) in a test environment, which is then evaluated for any indicators of compromise prior to authorization of production use

References

Source: https://pages.nist.gov/mobile-threat-catalogue/supply-chain-threats/SPC-3.html