APP-20 · Mobile Threat Catalogue

Archived: 2026-04-05 13:34:36 UTC

Mobile Threat Catalogue

Loading Malicious Code at Runtime

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-20

Threat Description: Mobile apps may evade app vetting by downloading and executing malicious app code after installation. On Android, external code can be loaded using the OS-provided API. On iOS, the ability to modify app code is a consequence of the Objective C runtime environment that apps execute within, which permits method definitions to be modified at runtime. As the malicious code would not be present when the app was submitted for review, it may evade detection as a malicious application.

Threat Origin

Execute This! Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications [1]

Jekyll on iOS: When Benign Apps Become Evil [2]

Exploit Examples

Android Hax [3]

Hot or Not? The Benefits and Risks of iOS Remote Hot Patching [4]

Method Swizzling [5]

CVE Examples

Possible Countermeasures

Enterprise

Deploy MAM or MDM solutions with policies that prohibit the side-loading of apps, which may bypass security checks on the app.

Deploy MAM or MDM solutions with policies that prohibit the installation of apps from 3rd party (unofficial) app stores.

Use application threat intelligence data about potential abuse of dynamic code execution associated with apps installed on COPE or BYOD devices

Mobile Device User

Use Android Verify Apps feature to identify potentially harmful apps.

Consider the use of devices that support Android 10 or higher, in which applications cannot execute code within their own system binaries and libraries.

References
