System Partition Integrity, Mitigation M1004 - Mobile

By Authorization Enforcement

Archived: 2026-04-05 18:24:39 UTC

Domain	ID		Name	Use
Mobile	T1398		Boot or Logon Initialization Scripts	Android and iOS include system partition integrity mechanisms that could detect unauthorized modifications.
Mobile	T1645		Compromise Client Software Binary	Android includes system partition integrity mechanisms that could detect unauthorized modifications.
Mobile	T1625		Hijack Execution Flow	Android Verified Boot can detect unauthorized modifications made to the system partition, which could lead to execution flow hijacking.[1]
		.001	System Runtime API Hijacking	Android Verified Boot can detect unauthorized modifications made to the system partition, which could lead to execution flow hijacking.[1]
Mobile	T1629		Impair Defenses	System partition integrity mechanisms, such as Verified Boot, can detect the unauthorized modification of system files.
		.003	Disable or Modify Tools	System partition integrity mechanisms, such as Verified Boot, can detect the unauthorized modification of system files.
Mobile	T1474	.003	Supply Chain Compromise: Compromise Software Supply Chain	Ensure Verified Boot is enabled on devices with that capability.

Source: https://attack.mitre.org/mitigations/M1004