Impair Defenses, Technique T1629 - Mobile

Archived: 2026-04-05 17:45:35 UTC

ID	Mitigation	Description
M1010	Deploy Compromised Device Detection Method	Mobile security software can typically detect if a device has been rooted or jailbroken and can inform the user, who can then take appropriate action.
M1012	Enterprise Policy	An EMM/MDM can use the Android `DevicePolicyManager.setPermittedAccessibilityServices` method to set an explicit list of applications that are allowed to use Android's accessibility features.
M1001	Security Updates	Security updates often contain patches for vulnerabilities that could be exploited for root access. Root access is often a requirement to impairing defenses.
M1004	System Partition Integrity	System partition integrity mechanisms, such as Verified Boot, can detect the unauthorized modification of system files.
M1011	User Guidance	Providing user guidance around commonly abused features, such as the modal that requests for administrator permissions, should aid in preventing impairing defenses.
