Detection of Code Signing Policy Modification, Detection Strategy DET0619

Archived: 2026-04-05 17:26:51 UTC

AN1679

On Android, the user can use the device settings menu to view trusted CA certificates and look for unexpected or unknown certificates. A mobile security product could similarly examine the trusted CA certificate store for anomalies. Users can use the device settings menu to view which applications on the device are allowed to install unknown applications.

On iOS, the user can use the device settings menu to view installed Configuration Profiles and look for unexpected or unknown profiles. A Mobile Device Management (MDM) system could use the iOS MDM APIs to examine the list of installed Configuration Profiles for anomalies.

Log Sources

AN1680

On Android, the user can use the device settings menu to view trusted CA certificates and look for unexpected or unknown certificates. A mobile security product could similarly examine the trusted CA certificate store for anomalies. Users can use the device settings menu to view which applications on the device are allowed to install unknown applications.

On iOS, the user can use the device settings menu to view installed Configuration Profiles and look for unexpected or unknown profiles. A Mobile Device Management (MDM) system could use the iOS MDM APIs to examine the list of installed Configuration Profiles for anomalies.

Log Sources
