Use Recent OS Version, Mitigation M1006 - Mobile

Archived: 2026-04-05 12:53:27 UTC

Mobile T1626 .001 Abuse Elevation Control Mechanism: Device Administrator Permissions

Changes were introduced in Android 7 to make abuse of device administrator permissions more difficult.[1]

Mobile T1638 Adversary-in-the-Middle

Recent OS versions have made it more difficult for applications to register as VPN providers.

Mobile T1661 Application Versioning

Android 11 and above implement application hibernation, which can hibernate an application that has not been used for a few months and can reset the application's permission requests.[2]

Mobile T1429 Audio Capture

Android 9 and above restricts access to microphone, camera, and other sensors from background applications.[3]

Mobile T1414 Clipboard Data

Android 10 introduced changes to prevent applications from accessing clipboard data if they are not in the foreground or set as the device's default IME.[4]

Mobile T1577 Compromise Application Executable

Many vulnerabilities related to injecting code into existing applications have been patched in previous Android releases.

Mobile T1641 Data Manipulation

Recent OS versions have limited access to certain APIs unless certain conditions are met, making Data Manipulation more difficult

.001 Transmitted Data Manipulation

Android 10 prevents applications from accessing clipboard data unless the application is on the foreground or is set as the device's default input method editor (IME).[4]

Mobile T1407 Download New Code at Runtime

Applications that target Android API level 29 or higher cannot execute native code stored in the application's internal data storage directory, limiting the ability of applications to download and execute native code at runtime. [5]

Mobile T1642 Endpoint Denial of Service

Android 7 changed how the Device Administrator password APIs function.

Mobile T1624 Event Triggered Execution

Android 8 introduced additional limitations on the implicit intents that an application can register for.[6]

.001 Broadcast Receivers

Android 8 introduced additional limitations on the implicit intents that an application can register for.[6]

Mobile T1627 Execution Guardrails

New OS releases frequently contain additional limitations or controls around device location access.

.001 Geofencing

New OS releases frequently contain additional limitations or controls around device location access.

Mobile T1420 File and Directory Discovery

Security architecture improvements in each new version of Android and iOS make it more difficult to escalate privileges. Additionally, newer versions of Android have strengthened the sandboxing applied to applications, restricting their ability to enumerate file system contents.

Mobile T1628 .001 Hide Artifacts: Suppress Application Icon

Android 10 introduced changes to prevent malicious applications from fully suppressing their icon in the launcher. [7][8]

Mobile T1629 .001 Impair Defenses: Prevent Application Removal

Recent versions of Android modified how device administrator applications are uninstalled, making it easier for the user to remove them.

.002 Impair Defenses: Device Lockout

Recent versions of Android modified how device administrator applications are uninstalled, making it easier for the user to remove them. Android 7 introduced updates that revoke standard device administrators' ability to reset the device's passcode.

Mobile T1417 Input Capture

The `HIDE_OVERLAY_WINDOWS` permission was introduced in Android 12 allowing apps to hide overlay windows of type `TYPE_APPLICATION_OVERLAY` drawn by other apps with the `SYSTEM_ALERT_WINDOW` permission, preventing other applications from creating overlay windows on top of the current application.[9]

.002 GUI Input Capture

The `HIDE_OVERLAY_WINDOWS` permission was introduced in Android 12 allowing apps to hide overlay windows of type `TYPE_APPLICATION_OVERLAY` drawn by other apps with the `SYSTEM_ALERT_WINDOW` permission, preventing other applications from creating overlay windows on top of the current application.[9]

Mobile T1430 Location Tracking

On Android 11 and up, users are not prompted with the option to select "Allow all the time" and must navigate to the settings page to manually select this option. On iOS 14 and up, users can select whether to provide Precise Location for each installed application.

Mobile T1424 Process Discovery

Android 7 and later iOS versions introduced changes that prevent applications from performing Process Discovery without elevated privileges.

Mobile T1636 Protected User Data

OS feature updates often enhance security and privacy around permissions.

.005 Accounts

OS feature updates often enhance security and privacy around permissions.

Mobile T1458 Replication Through Removable Media

iOS 11.4.1 and higher introduce USB Restricted Mode, which disables data access through the device's charging port under certain conditions (making the port only usable for power), likely preventing this technique from working.[10]

Mobile T1418 Software Discovery

Android 11 introduced privacy enhancements to package visibility, filtering results that are returned from the package manager. iOS 12 removed the private API that could previously be used to list installed applications on non-app store applications.[11]

.001 Security Software Discovery

Android 11 introduced privacy enhancements to package visibility, filtering results that are returned from the package manager. iOS 12 removed the private API that could previously be used to list installed applications on non-app store applications.[11]

Mobile T1635 Steal Application Access Token

iOS 11 introduced a first-come-first-served principle for URIs, allowing only the prior installed app to be launched via the URI.[12] Android 6 introduced App Links.

.001 URI Hijacking

iOS 11 introduced a first-come-first-served principle for URIs, allowing only the prior installed app to be launched via the URI.[12] Android 6 introduced App Links.

Mobile T1409 Stored Application Data

Android 9 introduced a new security policy that prevents applications from reading or writing data to other applications' internal storage directories, regardless of permissions.

Mobile T1632 Subvert Trust Controls

Mobile OSes have implemented measures to make it more difficult to trick users into installing untrusted certificates and configurations. iOS 10.3 and higher add an additional step for users to install new trusted CA certificates and configuration profiles. On Android, apps that target compatibility with Android 7 and higher (API Level 24) default to only trusting CA certificates that are bundled with the operating system, not CA certificates that are added by the user or administrator, hence decreasing their susceptibility to successful adversary-in-the-middle attack.[13][14]

.001 Code Signing Policy Modification

Mobile OSes have implemented measures to make it more difficult to trick users into installing untrusted certificates and configurations. iOS 10.3 and higher add an additional step for users to install new trusted CA certificates and configuration profiles. On Android, apps that target compatibility with Android 7 and higher (API Level 24) default to only trusting CA certificates that are bundled with the operating system, not CA certificates that are added by the user or administrator, hence decreasing their susceptibility to successful adversary-in-the-middle attack.[13][14]

Mobile T1422 System Network Configuration Discovery

Android 10 introduced changes that prevent normal applications from accessing sensitive device identifiers.[15]

.002 Wi-Fi Discovery

Android 10 introduced changes that prevent normal applications from accessing sensitive device identifiers.[15]

Mobile T1512 Video Capture

Android 9 and above restricts access to the mic, camera, and other device sensors from applications running in the background. iOS 14 and Android 12 introduced a visual indicator on the status bar (green dot) when an application is accessing the device's camera.[3]
