Protected User Data: Calendar Entries, Sub-technique T1636.001 - Mobile

Archived: 2026-04-05 16:40:19 UTC

ID	Name	Analytic ID	Analytic Description
DET0674	Detection of Calendar Entries	AN1774	Application vetting services could look for `android.permission.READ_CALENDAR` or `android.permission.WRITE_CALENDAR` in an Android application's manifest, or `NSCalendarsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need calendar access, so extra scrutiny could be applied to those that request it. On both Android and iOS, the user can manage which applications have permission to access calendar information through the device settings screen, revoke the permission if necessary.
		AN1775	Application vetting services could look for `android.permission.READ_CALENDAR` or `android.permission.WRITE_CALENDAR` in an Android application's manifest, or `NSCalendarsUsageDescription` in an iOS application's `Info.plist` file. Most applications do not need calendar access, so extra scrutiny could be applied to those that request it. On both Android and iOS, the user can manage which applications have permission to access calendar information through the device settings screen, revoke the permission if necessary.

Source: https://attack.mitre.org/techniques/T1636/001