

File and Directory Discovery, Technique T1420 - Mobile

Archived: 2026-04-05 18:24:56 UTC

Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Adversaries may use the information from [File and Directory Discovery](#) during automated discovery to shape follow-on behaviors, including deciding if the adversary should fully infect the target and/or attempt specific actions.

On Android, Linux file permissions and SELinux policies typically stringently restrict what can be accessed by apps without taking advantage of a privilege escalation exploit. The contents of the external storage directory are generally visible, which could present concerns if sensitive data is inappropriately stored there. iOS's security architecture generally restricts the ability to perform any type of [File and Directory Discovery](#) without use of escalated privileges.

Source: <https://attack.mitre.org/techniques/T1420>