Detection of Steal Application Access Token, Detection Strategy DET0656

Archived: 2026-04-05 14:52:54 UTC

AN1743

When vetting applications for potential security weaknesses, the vetting process could look for insecure use of Intents. Developers should be encouraged to use techniques to ensure that the intent can only be sent to an appropriate destination (e.g., use explicit rather than implicit intents, permission checking, checking of the destination app's signing certificate, or utilizing the App Links feature). For mobile applications using OAuth, encourage use of best practice.[1][2]
On Android, users may be presented with a popup to select the appropriate application to open a URI in. If the user sees an application they do not recognize, they can remove it.

Log Sources

AN1744

When vetting applications for potential security weaknesses, the vetting process could look for insecure use of Intents. Developers should be encouraged to use techniques to ensure that the intent can only be sent to an appropriate destination (e.g., use explicit rather than implicit intents, permission checking, checking of the destination app's signing certificate, or utilizing the App Links feature). For mobile applications using OAuth, encourage use of best practice.[1][2]
On Android, users may be presented with a popup to select the appropriate application to open a URI in. If the user sees an application they do not recognize, they can remove it.

Log Sources
