AUT-10 · Mobile Threat Catalogue

Archived: 2026-04-06 03:19:41 UTC

Mobile Threat Catalogue

Capturing Credentials

Contribute

Threat Category: Authentication: User or Device to Remote Service

ID: AUT-10

Threat Description: Malicious applications can intercept and steal passwords when logging in using webpages rendered within applications.

Threat Origin

OAuth 2.0 for Native Apps [1]

Exploit Examples

Stealing Passwords is Easy in Native Mobile Apps Despite OAuth [2]

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

Deploy MAM or MDM solutions with policies that prohibit the side-loading of apps, which may bypass security checks on the app.

Deploy MAM or MDM solutions with policies that prohibit the installation of apps from 3rd party (unofficial) app stores.

Use app-vetting tools or services to identify malicious behaviors in apps.

References

1. W. Denniss and J. Bradley, “OAuth 2.0 for Native Apps”, IETF Internet Draft, work in progress, July 2016; https://datatracker.ietf.org/doc/html/draft-wdenniss-oauth-native-apps [accessed 8/1/2022] ↩

2. A. Wulf, “Stealing Passwords is Easy in Native Mobile Apps Despite OAuth”, blog, 12 Jan. 2011; http://welcome.totheinter.net/2011/01/12/stealing-passwords-is-easy-in-native-mobile-apps-despite-oauth/ [accessed 8/25/2016] ↩
