APP-32 · Mobile Threat Catalogue

Archived: 2026-04-05 19:21:18 UTC

Mobile Threat Catalogue

Exploiting Access to Enterprise Resources

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-32

Threat Description: Any device-wide communication channels, such as an encrypted enterprise Wi-Fi connection, may be accessible to all apps running on the device. This may allow an attacker to bypass some network defense mechanisms, such as network access control or firewalls, thereby facilitating attacks against enterprise resources from within the enterprise network.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

Juniper Networks Third Annual Mobile Threats Report [1]

CVE Examples

- CVE-2016-10292

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 apps that perform host discovery or attempt to access hosts with internal (e.g. inside a private LAN) domains or IP addresses.

Use features such as Apple iOS Managed Apps, Android for Work, or Samsung KNOX Workspace that provide some level of separation between personal apps and enterprise apps to mitigate the impact of malicious behaviors,

including use of per-app/per-user VPN features, so that only enterprise-approved apps can traverse the VPN and access enterprise resources.

Mobile Device User

Use Android Verify Apps feature to identify potentially harmful.

References
