ECO-12 · Mobile Threat Catalogue

Archived: 2026-04-06 01:54:29 UTC

Mobile Threat Catalogue

Man in the Middle Attack on Application Download

Contribute

Threat Category: Mobile Application Store

ID: ECO-12

Threat Description: An attacker able to successfully execute a man in the middle attack on a connection could intercept legitimate application requests, and return back malicious or illegitimate applications to the user.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

Not Applicable

CVE Examples

Not Applicable

Possible Countermeasures

Enterprise

To decrease the time to detection, use app threat intelligence data to identify malicious applications installed on devices

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

To reduce the probability that an attacker will have established a MiTM on a session during which a user attempts to intall apps from a trusted source (e.g., official app store), recommend or require users to download apps when connected to a trusted and secured Wi-Fi network.

To reduce the probability that malicious apps will be installed on managed devices, use app-vetting tools or services in combination with MAM solutions to push vetted apps directly onto enrolled devices over trusted and secured Wi-Fi networks.

References

Source: https://pages.nist.gov/mobile-threat-catalogue/ecosystem-threats/ECO-12.html