APP-22 · Mobile Threat Catalogue

Archived: 2026-04-06 00:18:12 UTC

Mobile Threat Catalogue

Avoiding Uninstallation via Permissions Abuse

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-22

Threat Description: The Device Administrator permission in Android is designed to allow enterprises to develop apps that can manage settings on users devices to enforce compliance with the enterprise mobile device security policy. Prior to Android 6.0, the Device Administrator role could enforce a policy that disabled uninstallation of an app. Malicious applications could abuse this behavior to gain persistence on the device. Since Android 6.0, users can always unregister a given app as a Device Administrator, which disables all associated policies and would restore the ability to uninstall the malicious app.

Threat Origin

Android Security 2015 Year In Review [1]

Exploit Examples

Not Applicable

CVE Examples

- CVE-2017-0594
- CVE-2017-0595
- CVE-2017-0596

Possible Countermeasures

Enterprise

Ensure Android devices are running a recent version of the operating system. As described at 44:20 in the Google I/O 2016 “What’s new in Android security” (https://www.youtube.com/watch?v=XZzLjllizYs), enhancements were made in Android M or N to ensure that all device admin apps can be uninstalled.

Mobile Device User

Ensure Android devices are running a recent version of the operating system. As described at 44:20 in the Google I/O 2016 “What’s new in Android security” (https://www.youtube.com/watch?v=XZzLjllizYs), enhancements were made in Android M or N to ensure that all device admin apps can be uninstalled.

References

1. Android Security 2015 Year In Review, Google, 2016; https://source.android.com/security/reports/Google_Android_Security_2015_Report_Final.pdf [accessed 8/25/2016] ↩
