APP-27 · Mobile Threat Catalogue

Archived: 2026-04-05 19:42:08 UTC

Mobile Threat Catalogue

Persistance via Writing to System Partition

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-27

Threat Description: Malicious code that has achieved privilege escalation to the kernel or root user may achieve persistence by modifying memory locations reserved for use by the bootloader, mobile OS, or kernel to force the execution of malicious code following a device reboot or integrated factory reset.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

Brain Test re-emerges: 13 apps found in Google Play [1]

CVE Examples

- CVE-2016-10277

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 application threat intelligence data about apps that may achieve malicious persistence

Use app-vetting tools or services to identify apps that exploit the underlying OS to achieve malicious persistence.

Deploy MDM solutions that require successful boot attestation prior to granting access to enterprise resources.

Mobile Device User

Use Android Verify Apps feature to identify potentially harmful apps.

Mobile App Developer

To avoid executing apps that process sensitve information while low-level malware is present on the device, perform device integrity checking within enterprise applications, such as use of Android SafetyNet, Samsung Knox hardware-backed remote attestation, or other applicable remote attestation technologies device integrity attestation API

References
