APP-40 · Mobile Threat Catalogue

Archived: 2026-04-05 20:21:09 UTC

Mobile Threat Catalogue

Capturing Raw Screen Buffer

Contribute

Threat Category: Malicious or privacy-invasive application

ID: APP-40

Threat Description: A malicious application that has elevated to root privileges may be able to capture the contents of the screen buffer, in essence taking a screenshot of any foreground activity. This would allow an attacker to steal authentication credentals or gain unauthorized access to any other sensitive information displayed in the foreground. Note that this capture would not be handled like a user-initiated screenshot, and would not automatically be stored in default locations read by camera or photo browser apps (e.g. Google Photos).

Threat Origin

An investigation of Chrysaor Malware on Android [1]

Exploit Examples

An investigation of Chrysaor Malware on Android [1]

CVE Examples

Possible Countermeasures

Mobile Device User

To limit the opportunity for an attacker to realize this threat following a security patch for a priviledge escalation vulnerability, ensure timely installation of mobile OS security updates.

To reduce the probability of installing a malicious application, obtain public apps from an official app store (e.g., Google Play, iTunes Store).

On Adroid, to prevent an attacker from remotely installing 3rd party malicious apps, ensure Security > Unknown Sources is turned off.

To detect malicious applications, use on-device agents that automatically perform signature- and/or behavior-based malware detection.

Enterprise

To limit the opportunity for an attacker to realize this threat following a security patch for a priviledge escalation vulnerability, ensure timely installation of mobile OS security updates.

To prevent users of managed Android devices from installing applications from unknown sources, deploy EMM solutions that effectively disable the Unknown Sources feature.

To detect malicious applications, use on-device agents that automatically perform signature- and/or behavior-based malware detection.

To prevent granting access to compromised devices, use tools or device APIs (Android SafetyNet, Samsung Knox hardware-backed remote attestation, or other applicable remote attestation technologies) to detect and block enterprise connectivity from devices that fail attestation or integrity checks.

References
