APP-3 · Mobile Threat Catalogue

Archived: 2026-04-05 15:26:54 UTC

Mobile Threat Catalogue

Sensitive Information in System Logs

Contribute

Threat Category: Vulnerable Applications

ID: APP-3

Threat Description: Mobile application developers may unintentionally expose sensitive information by storing it in system logs designed to troubleshoot problems. An example would be logging the username and password for a failed user-to-app authentication attempt. An attacker with access to the system log would gain unauthorized access to the information.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

CVE Examples

- CVE-2012-2630
- CVE-2014-0647

Possible Countermeasures

Mobile App Developer

Avoid logging sensitive data in an unencrypted state, even to files internal to the app, as these files may be exposed in backups or direct access to the device’s file system.

Use the Compatibility Test Suite, which checks for the presence of potentially sensitive information in the system logs; See https://source.android.com/security/overview/implement.html.

Enterprise

Consider the use of devices that support Android 4.1 or later, in which apps can no longer access the system log (other than reading log entries added by the app itself).

Use app-vetting tools or services to identify apps that store sensitive information in system logs or other unsecure storage locations.

Mobile Device User

Consider the use of devices that support Android 4.1 or later, in which apps can no longer access the system log (other than reading log entries added by the app itself).

References
