Google LLC

Mobile Application Security Assessment

Device Health Services

05/29/2025 - Product Version - 1.27.0.711344205

SCOPE VERIFIED:

Device Health Services

DATE OF COMPLETION

May 29, 2025

Device Health Services

LEVIATHAN SECURITY GROUP

Test Results	All the requirements were met.	Pass

PACKAGE NAME	**com.google.android.apps.turbo**
TITLE	Device Health Services
DEVELOPER	Google LLC
SHA-256 HASH	b6de6f8fa0276d432b8e23d5028ba1da8c82231d79d53c10c2dbdfd44207cb91
SIZE	11.6MB
VERSION CODE	10270892
VERSION NAME	1.27.0.711344205
DEVICE	Google Pixel 7
API LEVEL	35
ASSURANCE LEVEL	AL2 - Lab Tested
SPECIFICATION VERSION	1.0

Test Background

The Open Web Application Security Project (OWASP) has been around for over 20 years and has helped provide a much more secure experience for both web and mobile users. More recently, it published the Mobile Application Security Verification Standard (MASVS), which aims to define a common standard for secure mobile applications. With the App Defense Alliance, Google has brought together application developers and independent security labs in an effort to improve the security of mobile application security and highlight those apps that meet the standard. The security labs verify the applications against specific MASVS requirements and work with developers to address any issues.

OWASP also publishes the Mobile Security Testing Guide (MSTG), which details how the application should be tested, and provides information to developers on how to write more secure applications. The following section it taken directly from the MSTG to highlight current security best practices, as well as link to additional resources for application developers.

The scope of this work was limited to the specific requirements of the Application Defense Alliance described below and should not be read as a holistic security evaluation or comprehensive penetration test.

Passed Requirements

CATEGORY	STATUS
Storage	
The application securely stores sensitive data in external storage	Pass
The application prevents leakage of sensitive data	Pass
Crypto	
The application employs current strong cryptography and uses it according to industry best practices	Pass
The application performs key management according to industry best practices	Pass
Auth	
The application uses secure authentication and authorization protocols and follows the relevant best practices	Pass
Network	
The application secures all network traffic according to the current best practices	Pass
Platform	
The application uses IPC mechanisms securely	Pass
The application uses WebViews securely	Pass
The application uses the user interface securely	Pass

Code	
The application requires an up-to-date platform version	Pass
The application only uses software components without known vulnerabilities	Pass
The application validates and sanitizes all untrusted inputs	Pass
Resilience	
The application implements anti-tampering mechanisms	Pass
The application implements anti-static analysis mechanisms	Pass
The application implements anti-dynamic analysis mechanisms	Pass
Privacy	
The application minimizes access to sensitive data and resources	Pass
The application is transparent about data collection and usage	Pass
The application offers user control over their data	Pass