SurfShark VPN Assessment

Google LLC
January 22th, 2025 - 3.11.2
com.surfshark.vpnclient.android

VPN®

NowSecure™

The following assessment was performed using the OWASP Mobile Application Security Verification Standard (MASVS) version 1.4, with the test guidance from OWASP Mobile Security Testing Guide (MSTG) version 1.3. Full specifications can be found on GitHub here.

Category	Status	Justification
Architecture, Design and Threat Modeling Requirements (MSTG-ARCH-2)	Pass	Security controls were enforced on the remote endpoint. Software updates are provided by the developer and deployed through the Google Play Store. The developer maintains a vulnerability disclosure program which can be found at this link.
Data Storage and Privacy Requirements (MSTG-STORAGE-1, MSTG-STORAGE-2, MSTG-STORAGE-3, MSTG-STORAGE-5, MSTG-STORAGE-7, MSTG-STORAGE-12)	Pass	The developer protected sensitive data using industry recommended best practices. No sensitive data storage outside the application container or logs were detected during testing. The developer declarations on the security and privacy label are accurate and understandable by the user.
Cryptography Requirements (MSTG-CRYPTO-1, MSTG-CRYPTO-2, MSTG-CRYPTO-3, MSTG-CRYPTO-4, MSTG-CRYPTO-5, MSTG-CRYPTO-6)	Pass	The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices. The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes.
Authentication and Session Management Requirements (MSTG-AUTH-1, MSTG-AUTH-2, MSTG-AUTH-3, MSTG-AUTH-4, MSTG-AUTH-5, MSTG-AUTH-6, MSTG-AUTH-7)	Pass	The app and remote endpoint implemented authentication methods which followed the guidelines from OWASP MASVS. Bruteforce mitigations were in place at the remote endpoint and session tokens were managed in a secure manner.
Network Communication Requirements (MSTG-NETWORK-1, MSTG-NETWORK-2, MSTG-NETWORK-3)	Pass	The app only depends on up-to-date connectivity and security libraries. Communications with the remote endpoint are protected using TLS with settings in line with current best practices. The app only accepted valid certificates.
Platform Interaction Requirements (MSTG-PLATFORM-1, MSTG-PLATFORM-2, MSTG-PLATFORM-3, MSTG-PLATFORM-4)	Pass	The app only requested the minimum set of permissions necessary and did not export sensitive functionality. Inputs from external sources and the user were validated.

Code Quality and Build Setting Requirements (MSTG-CODE-1, MSTG-CODE-2, MSTG-CODE-3, MSTG-CODE-4, MSTG-CODE-5, MSTG-CODE-9)	Pass	The application was built in release mode with debugging symbols removed using the default security compiler settings.

Assumptions

Application testing was conducted on NowSecure instrumented devices that have been jailbroken/rooted. This affords the analysts the greatest level of coverage. While the mobile operating system can offer mitigating controls for application security, in most situations it is best practice for the application to secure its own data as much as possible, making the assumption that it is operating on a compromised device.