Mobile Application Security Assessment (MASA) Letter of Assessment (LOA) for: Mullvad VPN v2024.9

Google

Version 1.0 – February 24, 2025

1 MASA Letter of Assessment

In February of 2025, NCC Group performed a Mobile Application Security Assessment (MASA) against Mullvad VPN v2024.9 (the "**Application**") for and on behalf of Google LLC ("**Developer**") pursuant to the governing contract(s) between NCC Group and Developer. The assessment objective was to identify compliance with the MASA framework within a time-boxed assessment. MASA is defined by the App Defense Alliance (ADA) and is based on the OWASP Mobile Application Security Verification Standard (MASVS). For more specific information on the specific requirements assessed, please see Appendix A.

This Letter of Assessment ("**LOA**") confirms that the assessment of the Application has been completed and was found to substantially comply with the requirements in Appendix A.

It is important to note that this LOA represents a point-in-time evaluation. The security and compliance of an application can evolve rapidly, and the results of this assessment are not intended to represent an endorsement of the Application's future compliance or adequacy of current security measures against future threats. This LOA necessarily contains information in summary form and is therefore intended for general guidance only; it is not intended as a substitute for detailed research or the exercise of professional judgment. The information presented here should not be construed as professional advice or service.

Technical Constraints

The following items may impact the completeness and accuracy of the test case results:

- The MASA framework was in active development during the assessment. Some controls may have been modified during or after the testing period.
- Some controls employed ambiguous language. When presented with equally valid interpretations of a control, NCC Group selected the strictest version unless otherwise directed by Google.

Terms, Limitations and Disclaimers

- Prepared by NCC Group Security Services, Inc. for Developer.
- Portions of this document and the templates used in its production are the property of NCC Group and cannot be copied or disclosed (in full or in part) without NCC Group's prior written permission.
- While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein.
- NCC Group provides no warranty or guarantee that any of NCC Group's services including but not limited to, recommendations, results or assessments will prevent or avoid any future security breaches or unauthorized access to the Application or Developer's networks or systems.
- MASA is intended to provide more transparency into application security, however the limited nature of testing does not guarantee complete safety of the Application. This independent review may not be scoped to verify the accuracy and completeness of a developer's data safety declarations. Developer remains solely responsible for making complete and accurate declarations in their app's Google listings.
- NCC Group further expressly disclaims all warranties and conditions of any kind, whether express or implied, including, but not limited to the implied warranties and conditions of merchantability, fitness for a particular purpose and non-infringement.

APPENDIX A: MASA Requirements as Tested

Requirements used for this LOA are outlined below. These are based on ADA MASA version 1.5 dated 7/13/2022 per the Application Defense Alliance Mobile Security Guide (ADAMSG). Where there are differences between below requirements and ADAMSG, the below requirements were followed.

The "MSTG-ID" column refers to the related OWASP Mobile Application Security Testing Guide (MASTG, previously known as Mobile Security Testing Guide, MSTG) requirements upon which the listed MASA requirement is based.

Legend:

- **PASS** = NCC Group did not observe significant non-compliance with the indicated MASA Requirement during testing.
- **FAIL** = NCC Group observed significant non-compliance with the indicated Requirement during testing.
- **INC** = "Inconclusive," NCC Group was unable to verify compliance with the indicated Requirement either due to ambiguity in observed evidence or of the Requirement itself. This is effectively a FAIL from an overall LOA standpoint.
- **NA** = "Not Applicable," NCC Group judged the Requirement to be inapplicable to the target application. This is effectively a PASS from an overall LOA standpoint.

ID	MSTG-ID	Description	Status
V2: Data Storage and Privacy Requirements			
2.1	MSTG-STORAGE-1	System credential storage facilities need to be used to store sensitive data, such as PII, user credentials or cryptographic keys.	Pass
2.2	MSTG-STORAGE-2	No sensitive data should be stored outside of the app container or system credential storage facilities.	Pass
2.3	MSTG-STORAGE-3	No sensitive data is written to application logs.	Pass
2.5	MSTG-STORAGE-5	The keyboard cache is disabled on text inputs that process sensitive data.	Pass
2.7	MSTG-STORAGE-7	No sensitive data, such as passwords or pins, is exposed through the user interface.	Pass
2.12	MSTG-STORAGE-12	The app educates the user about the types of personally identifiable information processed, as well as security best practices the user should follow in using the app.	Pass
V3: Cryptography Requirements			
3.1	MSTG-CRYPTO-1	The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	Pass
3.2	MSTG-CRYPTO-2	The app uses proven implementations of cryptographic primitives.	Pass

ID	MSTG-ID	Description	Status
3.3	MSTG-CRYPTO-3	The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.	Pass
3.4	MSTG-CRYPTO-4	The app does not use cryptographic protocols or algorithms that are widely considered deprecated for security purposes.	Pass
3.5	MSTG-CRYPTO-5	The app does not re-use the same cryptographic key for multiple purposes.	Pass
3.6	MSTG-CRYPTO-6	All random values are generated using a sufficiently secure random number generator.	Pass
V4: Authentication and Session Management Requirements			
4.1	MSTG-AUTH-1	If the app provides users access to a remote service, some form of authentication, such as username/ password authentication, is performed at the remote endpoint.	Pass
4.2	MSTG-AUTH-2	If stateful session management is used, the remote endpoint uses randomly generated session identifiers to authenticate client requests without sending the users credentials.	Pass
4.3	MSTG-AUTH-3	If stateless token-based authentication is used, the server provides a token that has been signed using a secure algorithm.	Pass
4.4	MSTG-AUTH-4	The remote endpoint terminates the existing session when the user logs out.	Pass
4.5	MSTG-AUTH-5	A password policy exists and is enforced at the remote endpoint.	Pass
4.6	MSTG-AUTH-6	The remote endpoint implements a mechanism to protect against the submission of credentials an excessive number of times.	Pass
4.7	MSTG-AUTH-7	Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access tokens expire.	Pass
V5: Network Communication Requirements			
5.1	MSTG-NETWORK-1	Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.	Pass
5.2	MSTG-NETWORK-2	The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.	Pass

ID	MSTG-ID	Description	Status
5.3	MSTG-NETWORK-3	The app verifies the X.509 certificate of the remote endpoint when the secure channel is established. Only certificates signed by a trusted CA are accepted.	Pass
V6: Platform Interaction Requirements			
6.1	MSTG-PLATFORM-1	The app only requests the minimum set of permissions necessary.	Pass
6.2	MSTG-PLATFORM-2	All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.	Pass
6.3	MSTG-PLATFORM-3	The app does not export sensitive functionality via custom URL schemes unless these mechanisms are properly protected.	Pass
6.4	MSTG-PLATFORM-4	The app does not export sensitive functionality through IPC facilities, unless these mechanisms are properly protected.	Pass
V7: Code Quality and Build Setting Requirements			
7.1	MSTG-CODE-1	The app is signed and provisioned with a valid certificate, of which the private key is properly protected.	Pass
7.2	MSTG-CODE-2	The app has been built in release mode, with settings appropriate for a release build (e.g., non-debuggable).	Pass
7.3	MSTG-CODE-3	Debugging symbols have been removed from native binaries.	Pass
7.4	MSTG-CODE-4	Debugging code and developer assistance code (e.g., test code, backdoors, hidden settings) have been removed. The app does not log verbose errors or debugging messages.	Pass
7.5	MSTG-CODE-5	All third-party components used by the mobile app, such as libraries and frameworks, are identified, and checked for known vulnerabilities.	Pass
7.9	MSTG-CODE-9	Free security features offered by the toolchain, such as byte-code minification, stack protection, PIE support and automatic reference counting, are activated.	Pass