SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Report 1909090

Security Assessment ProtonVPN macOS App

for

Proton Technologies AG

conducted by

SEC Consult

Version: 1.2 | **Date:** 2019-11-22
Responsible: SEC Consult | **Author**: SEC Consult
Confidentiality class: Public

Table of Contents

1 Management Summary

The following chapter summarizes the scope of the audit, the results of the audit and outlines the measures recommended by SEC Consult.

1.1 Scope and Timetable

During the initial security assessment for Proton Technologies AG, SEC Consult performed a source code review of the ProtonVPN client for macOS - a VPN app for desktops running macOS, which offers private and secure passing of user traffic through Secure Core network in privacy-friendly countries like Switzerland and Iceland. Objective of the review was to reveal security issues and to offer suggestions for improvement. The focus of the code review was to provide answers to the following questions:

- Does the ProtonVPN solution ensure the privacy of the user?
- Is an attacker able to access data of other customers (cross-tenant access)?
- Is an attacker able to use paid ProtonVPN features without an account upgrade?

The review was conducted in August 2019 and a total effort of 6 days was dedicated to identifying and documenting security issues in the code base of the ProtonVPN Windows App.

Version 1.5.8 (Build 1089) of the application was tested. Full access to the source code was granted and test user credentials of the roles “free”, “plus”, “professional”, and “visionary” were provided.

The following files and documents were made available in the course of the review:

Files	SHA1 Sum
Proton Technologies.zip	95fa0c89296d5de434919eefade89f35c73c9015
ProtonVPN-macOS.zip	3e3e50914f6bfc2ee2f002a4c13172aef550fb06
ProtonVPN cert pinning OFF.dmg	e4684fb032f860dfd8e5b935d1a126b1109bf126
ProtonVPN.dmg	6d7d76c36cce2486a20fcd2c7106b424454efb74
README.md	752bd835feab69d394223e40333c8474b9bc4cc8

1.2 Results

During the initial code review, SEC Consult found no vulnerabilities in the reviewed source code and the macOS app within the given timeframe.

No issues have been identified that would allow an attacker to break ProtonVPN's encryption or to access other customers' data.

1.3 Disclaimer

At the request of Proton Technology AG, this report has been declassified from strictly confidential to public. While the report was shortened for public release, relevant vulnerability information has been maintained.

In this particular project, a timebox approach was used to define the consulting effort. This means that SEC Consult allotted a prearranged amount of time to identify and document vulnerabilities. Because of this, there is no guarantee that the project has discovered all possible vulnerabilities and risks.

Furthermore, the security check is only an immediate evaluation of the situation at the time the check was performed. An evaluation of future security levels or possible future risks or vulnerabilities may not be derived from it.

2 Vulnerability Summary

This chapter contains all identified vulnerabilities in the assessed macOS application of the company Proton Technologies AG.

Risk assessment	Initial no. of vulnerability classes	Current no. of vulnerability classes
Low	0	0
Medium	0	0
High	0	0
Critical	0	0
Total	**0**	**0**

2.1 Total Risk Per System

The following table contains a risk assessment for each system which contained security flaws.

System	Field of application	Initial risk	Current risk
ProtonVPN macOS Application	ProtonVPN macOS App	-	-
Total	**-**	**-**	**-**

3 Detailed Analysis

This chapter outlines the attacks and found vulnerabilities in detail.

3.1 ProtonVPN macOS Application Security Audit

3.1.1 General Information

ProtonVPN for macOS is designed for macOS devices and provides a virtual private network (VPN) service capabilities to their end users. During the timeframe of the review, the ProtonVPN macOS App was tested using a MacBook Pro running macOS Mojave. The tested macOS app is written in Swift and Objective-C.

All findings in the initial assessment were related to the API endpoints and have been merged with the dedicated API security review Report.

The applications source code files were checked against hardcoded credentials, which could potentially allow an attacker to bypass the authentication provider that has been configured by the software administrator. However, no hardcoded credentials were found in the source code.

The code was then reviewed according to multiple best practice and security guidelines, checking for common and potential security issues in the methods and procedures used and the design and implementation of the code.

Many areas of good security practice were seen in the code and the macOS version of ProtonVPN. The code was well written and followed best practise with regards to the code structure, commenting and readability including following the Model-View-View-Model-Coordinator (MVVM-C) architectural pattern.

4 Version History

Version	Date	Status/Changes	Created by	Responsible
1.0	2019-09-03	Initial report	SEC Consult	SEC Consult
1.2	2019-11-22	Public report	SEC Consult	SEC Consult