SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Report 1909090

Security Assessment ProtonVPN iOS 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 iOS - a VPN app for Apple devices, 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 initial 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 Android App.

Version 2.0.0 (Build 1028) 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
ProtonVPN-iOS.zip	fb51c837918b1ad583f89c5999e4945981df9d8c
ProtonVPN.ipa	9f8473c55991fe0c49654220a3d7d1d27650a02d
ProtonVPN cert pinning OFF.ipa	31ff2ad8e5a570dbdf727ffd714fa7272582047c
README.md	752bd835feab69d394223e40333c8474b9bc4cc8

In October 2019, Proton Technologies AG fixed the identified issues and supplied the fixes to SEC Consult for verification. Goal of the fix verification was to confirm remediation provided by the applied fixes. SEC Consult verified the fixes in November 2019.

1.2 Results

During the initial code review, SEC Consult found two **low-risk vulnerabilities** in the reviewed source code and the mobile app.

Although issues with certificate validation have been identified within the encrypted communication between the mobile application and the backend system, encrypted VPN traffic could not be decrypted.

No issues were identified, which would provide an attacker unauthorized access to other customers' data without having physical access to the victim's device.

All security issues that were identified in the initial security assessment was properly fixed or accepted by Proton Technologies AG.

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 reviewed source code of the company Proton Technologies AG.

Risk assessment	Initial no. of vulnerability classes	Current no. of vulnerability classes
Low	2	0
Medium	0	0
High	0	0
Critical	0	0
Total	**2**	**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 iOS Application	ProtonVPN iOS App	Low	-
Total	**-**	**Low**	**-**

2.2 Risk of Each Vulnerability

The following table contains a risk assessment for the discovered vulnerabilities.

Vulnerability	System	Initial risk	Current risk	Page
Mobile App Does Not Use SSL Certificate Pinning	ProtonVPN iOS App	Low	FIXED	6
Mobile App Runs on Jailbroken or Rooted Device	ProtonVPN iOS App	Low	ACCEPTED	7
Total	**-**	**Low**	**-**	**-**

3 Detailed Analysis

This chapter outlines the attacks and found vulnerabilities in detail.

3.1 ProtonVPN iOS Application Security Audit

3.1.1 General Information

This section describes vulnerabilities found in the ProtonVPN iOS Application.

ProtonVPN for iOS is designed for mobile devices and provides virtual private network (VPN) service capabilities to mobile users. During the timeframe of the review, the ProtonVPN iOS App was tested using a Jailbroken iPhone with iOS 12.3. The tested iOS app is written in Swift and Objective-C.

3.1.2 Mobile App Does Not Use SSL Certificate Pinning – FIXED

The mobile application did not check that the SSL certificate presented by the server was the one that was expected. This could allow an attacker to intercept or tamper with communications. The SSL certificate of the API server should be pinned within the application.

CVSS-v3 Base Score: 3.7 (Low)

CVSS-v3 Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

3.1.2.1 Recheck result

During the fix verification it was not possible for an attacker to intercept and manipulate the communication between the mobile app and the backend server. Certificates are properly validated now.

3.1.3 Mobile App Runs on Jailbroken or Rooted Device - ACCEPTED

It was possible to run the application on a jailbroken test device. This could allow a user or malicious app to access the app's sandbox, interfere with the app's communication, or extract data from the device.

Implement jailbreak detection code and alert the user if the device has been jailbroken.

CVSS-v3 Base Score: 3.0 (Low)

CVSS-v3 Vector String: CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N

3.1.3.1 Recheck results

The issue remained unchanged. However, the risk is accepted by Proton Technologies AG

Statement Proton Technologies AG:
We will not fix as there is no one solution to reliably detecting if an iOS device has been jailbroken or rooted. Furthermore, we expect users to be responsible for the security of their device once jailbroken or rooted.

4 Version History

Version	Date	Status/Changes	Created by	Responsible
1.0	2019-09-03	Initial report	SEC Consult	SEC Consult
1.1	2019-11-10	Fix verification	SEC Consult	SEC Consult
1.2	2019-11-22	Public report	SEC Consult	SEC Consult