SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Report 1907974

Source Code Review ProtonVPN Android App

for

Proton Technologies AG

conducted by

SEC Consult

Version: 1.2 | **Date:** 2019-11-15
Responsible: SEC Consult | **Author**: SEC Consult
Confidentiality class: Public

Table of Contents

1 Management Summary

The following chapter summarizes the scope and timetable of the code review, the results of the code review, 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 Android - a VPN app for Android 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 Q1 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 2.0.4 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
android-app-development.zip	2a01b63a37b335cf4d1e37b5a87dab866eb6b545
ProtonVPN-2.0.4(102)-prod-release.apk	3569c15655bae5b25c27d088613d38ca08ffeb35
Readme.md	368dbfbf2ed0e66426af14d5941ba45001ebfdf0

In September 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 October 2019.

1.2 Results

During the initial code review, SEC Consult found one **medium-risk vulnerability** and four **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. An attacker with physical access to a mobile device can obtain user-related information from debug routines, as excessive debug messages contain various user-related information that can be easily accessed by an attacker.

All security issues that were identified in the initial code review were 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	4	0
Medium	1	0
High	0	0
Critical	0	0
Total	**5**	**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 Android App	Mobile	Medium	-
Total	**-**	**Medium**	**-**

2.2 Risk of Each Vulnerability

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

Vulnerability	System	Initial risk	Current risk	Page
Insecure Logout	ProtonVPN Android App	Medium	FIXED	7
Debug Messages Enabled	ProtonVPN Android App	Low	ACCEPTED	8
Application Data Backup via ADB Enabled	ProtonVPN Android App	Low	FIXED	9
Hardcoded Credentials / Imperfect Data Encryption	ProtonVPN Android App	Low	ACCEPTED	10
Missing Certificate Pinning	ProtonVPN Android App	Low	FIXED	11
Total	**-**	**Medium**	**-**	**-**

3 Detailed Analysis

This chapter outlines the attacks and found vulnerabilities in detail.

3.1 ProtonVPN Android App

3.1.1 General Information

This section describes vulnerabilities found in the ProtonVPN Android App.

ProtonVPN Android App is designed for Android based mobile devices and provides VPN services to mobile users. During the timeframe of the audit the ProtonVPN Android App version 2.0.4 was tested using a rooted smartphone with Android OS 5.0. The tested Android application is written in Java, new functions are implemented in Kotlin.

3.1.2 Insecure Logout - FIXED

The ProtonVPN Android App does not perform a server-side logout after the mobile user clicks the logout button inside the mobile app. After the logout, the app user is redirected to the app login screen, but no logout request is sent to the server, therefore it is possible to reuse session/authentication tokens after the user logout.

CVSS-v3 Base Score: 4.8 (Medium)

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

3.1.2.1 Recheck results

During the fix verification it was not possible to reproduce the initial scenario. Upon logout, sessions were correctly terminated.

3.1.3 Debug Messages Enabled - ACCEPTED

The ProtonVPN Android App has debug messages enabled. It is a common practice to add debug routines to the code while developing an application. Often developers forget to remove these debug functions and deploy an application with enabled debugging features. During the audit timeframe it was identified that debug messages contain potentially sensitive data.

CVSS-v3 Base Score: 2.9 (Low)

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

3.1.3.1 Recheck results

The following output is an excerpt of the debug messages produced by the mobile application. Various information was observed in the log such as local internal IP address, local external IP address, OpenVPN/IKE2 username, detailed error stack traces:

```
[…]
09-06 15:04:21.917  7348  7690 I charon  : 14[ENC] generating IKE_AUTH
request 4 [ AUTH ]
09-06 15:04:21.918  7348  7690 I charon  : 14[NET] sending packet: from
192.168.0.159[46505] to 217.23.3.171[4500] (97 bytes)
09-06 15:04:21.957  7348  7691 I charon  : 15[NET] received packet: from
217.23.3.171[4500] to 192.168.0.159[46505] (321 bytes)
09-06 15:04:21.958  7348  7691 I charon  : 15[ENC] parsed IKE_AUTH response
4 [ AUTH CPRP(ADDR DNS) SA TSi TSr N(AUTH_LFT) N(MOBIKE_SUP) N(ADD_4_ADDR)
N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_4_ADDR)
N(ADD_4_ADDR) N(ADD_4_ADDR) ]
09-06 15:04:21.958  7348  7691 I charon  : 15[IKE] authentication of 'ikev2-
android' with EAP successful
09-06 15:04:21.959  7348  7691 I charon  : 15[IKE] IKE_SA android[1]
established between
192.168.0.159[RipOMGN2po6wGMEDUOMP1oFe]...217.23.3.171[ikev2-android]
09-06 15:04:21.959  7348  7691 I charon  : 15[IKE] scheduling rekeying in
35600s
[…]
```

Statement Proton Technologies AG:
All debug logs from within the Proton applications have been removed; the remaining output is generated by loggers outside of the control of the app itself (e.g. system logs). Information that is shown there is classified as low sensitivity. In the case of ProtonVPN applications, the VPN protocol credentials (for OpenVPN/IKEv2) are designed to be separate from a user's account credentials and are also classified as low sensitivity.

3.1.4 Application Data Backup via ADB Enabled - FIXED

The ProtonVPN Android App uses the default settings, where it allows a user to perform application data backup. An attacker may be able to obtain backup data, which might contain sensitive information, via ADB. Although several conditions have to be met prior to a successful attack such as an attacker gains physical access to the Android device where it has USB debugging enabled on it, these default settings are still considered as a security issue that may cause high impact if the attacker can successfully exploit.

CVSS-v3 Base Score: 2.1 (Low)

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

3.1.4.1 Recheck results

During the recheck audit the `android:allowBackup` attribute under the `<application>` tag in the AndroidManifest.xml file was found to be set to `"false"` as shown in the following snippet:

```
[…]
<application android:theme="@style/AppTheme"
android:label="@string/app_name" android:icon="@mipmap/ic_launcher"
android:name="com.protonvpn.android.ProtonApplication"
android:allowBackup="false" android:largeHeap="true"
android:supportsRtl="true"
android:networkSecurityConfig="@xml/network_security_config"
android:roundIcon="@mipmap/ic_launcher_round"
android:appComponentFactory="androidx.core.app.CoreComponentFactory">

<uses-library android:name=[…]
```

3.1.5 Hardcoded Credentials / Imperfect Data Encryption - ACCEPTED

The Android app stores user settings locally in the Shared Preferences file. The contents of the file are symmetrically encrypted using hardcoded keys together with the device identifier. Any attacker that has physical access to the device may obtain the encryption key from the decompiled app source code and decrypt user settings.

CVSS-v3 Base Score: 2.9 (Low)

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

3.1.5.1 Recheck results

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

Statement Proton Technologies AG:
These credentials are used to allow a client to send based exception reports (one way) to a logging system; additionally, the API endpoint for reporting is rare limited.

3.1.6 Missing Certificate Pinning - FIXED

Certificate Pinning allows mobile applications to verify that they are only connecting to a server over SSL/TLS which he is intended to. Furthermore, it is possible to verify, that the connection between client and server is end-to-end encrypted and not intercepted. This is ensured by embedding a hash of the server's certificate or a hash of the public key directly into the application.

During the process of establishing a connection to the server, the hash of the certificate/public key of the server is obtained and compared against the embedded hash of the certificate(s)/public key(s). If the retrieved hash of the certificate/public key is matching the locally stored hash of the certificate/public key the connection will be established, otherwise the connection will fail.

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

3.1.6.1 Recheck results

During the security assessment it was not possible for an attacker to intercept and manipulate the communication between the mobile app and the backend server:

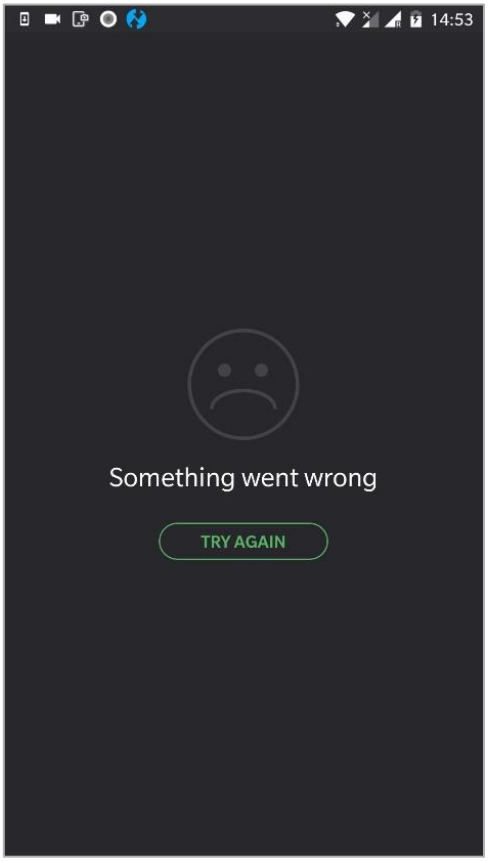

Figure 1. Certificate pinning is in place.

4 Version History

Version	Date	Status/Changes	Created by	Responsible
1.0	2019-03-15	Initial report	SEC Consult	SEC Consult
1.1	2019-10-10	Fix verification	SEC Consult	SEC Consult
1.2	2019-11-15	Public report	SEC Consult	SEC Consult