SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Report 1907974

Source Code Review ProtonVPN Windows 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 Windows - a VPN app for desktops running Windows, 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 Windows App.

Version 1.10.2 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.config	4376270dad7c01c9bab2010613801e2bd3c37389
README.md	4080a4817f7070152b01958bad0eb3a7a4d70190
Win-client.zip	eac6a053c0a3eb0b75d4e594abd1e1c3afd506df

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 two **medium-risk vulnerabilities** and two **low-risk vulnerabilities** in the reviewed source code and the app. However, it was not possible to decrypt encrypted VPN traffic.

No issues were identified, which would provide an attacker unauthorized access to other customers' data without having physical access to the victim's desktop. An attacker with physical access to a victim's desktop can obtain user-related information either from debug routines (excessive debug messages contain various user-related information that can be easily accessed by an attacker), or from memory dump of the application.

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	2	0
Medium	2	0
High	0	0
Critical	0	0
Total	**4**	**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 Windows App	Desktop	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
Sensitive Data in Memory	ProtonVPN Windows App	Medium	ACCEPTED	7
Hardcoded Credentials	ProtonVPN Windows App	Medium	ACCEPTED	8
Debug Messages Enabled	ProtonVPN Windows App	Low	FIXED	9
OpenVPN UDP Listener on All Interfaces	ProtonVPN Windows App	Low	FIXED	10
Total	**-**	**Medium**	**-**	**-**

3 Detailed Analysis

This chapter outlines the attacks and found vulnerabilities in detail.

3.1 ProtonVPN Windows App

3.1.1 General Information

This section describes vulnerabilities found in the ProtonVPN Windows App.

ProtonVPN Windows App provides VPN services to Windows OS users. During the timeframe of the audit the ProtonVPN Windows App version 1.10.2 was tested on a fully patched Windows 10 x64 machine. The tested Windows application is a .NET application written in C#.

3.1.2 Sensitive Data in Memory - ACCEPTED

The tested Windows app temporarily stores data in memory for various processing purposes. The stored data includes plain text session tokens and VPN credentials. If an attacker has access to the running ProtonVPN process, he may be able to dump memory contents and identify sensitive info stored in it.

CVSS-v3 Base Score: 6.1 (Medium)

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

3.1.2.1 Recheck results

During the tests the memory dump of a running ProtonVPN.exe process was obtained. While analyzing the contents of the memory dump a logged-in user's session token information and VPN username/password credentials in plain text (see figure below) were identified.

```
012C9FA0  0A 20 20 20 20 22 56 50  4E 22 3A 20 7B 0A 20 20     "VPN": {
012C9FB0  20 20 20 20 20 20 22 4E  61 6D 65 22 3A 20 22 52      "Name": "R
012C9FC0  69 70 4F 4D 47 4E 32 70  6F 36 77 47 4D 45 44 55 ipOMGN2po6wGMEDU
012C9FD0  4F 4D 50 31 6F 46 65 22  2C 0A 20 20 20 20 20 20 OMP1oFe",
012C9FE0  20 20 22 50 61 73 73 77  6F 72 64 22 3A 20 22 65   "Password": "e
012C9FF0  4B 74 43 53 54 44 56 56  33 62 58 34 74 37 72 49 KtCSTDVV3bX4t7rI
012CA000  37 68 42 56 49 69 59 22  2C 0A 20 20 20 20 20 20 7hBVIiY",
012CA010  20 20 22 45 78 70 69 72  61 74 69 6F 6E 54 69 6D   "ExpirationTim
012CA020  65 22 3A 20 30 2C 0A 20  20 20 20 20 20 20 20 22 e": 0,         "
012CA030  47 72 6F 75 70 49 44 22  3A 20 22 52 69 70 4F 4D GroupID": "RipOM
012CA040  47 4E 32 70 6F 36 77 47  4D 45 44 55 4F 4D 50 31 GN2po6wGMEDUOMP1
012CA050  6F 46 65 22 2C 0A 20 20  20 20 20 20 20 20 20 53 oFe",         "S
```

Figure 1. Plain text credentials in memory.

Such sensitive data was not destroyed after a user logout (after a logout the session tokens are invalidated, therefore the obtained plaintext session values would not create a risk), but only when the process is terminated the memory is wiped out.

Statement Proton Technologies AG:
.NET and Go garbage collectors are outside of our control and there is no way to deterministically force them to clear unused memory.

3.1.3 Hardcoded Credentials - ACCEPTED

The application source code files contain hardcoded credentials. This could potentially allow an attacker to bypass the authentication provider that has been configured by the software administrator. Usually, the existence of hardcoded credentials is not known to administrators. Once this security issue has been detected, it's not always trivial to mitigate it as the affected software may come in a binary form, so temporary solutions such as entirely disabling the affected software are involved.

CVSS-v3 Base Score: 4.0 (Medium)

CVSS-v3 Vector String: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/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:
The identified keys are classified not sensitive as we distribute them openly with our config files. The mentioned keys are OpenVPN TLS-auth keys which is used while establishing contact to a VPN server. It is not used for the authentication of either server to client or vice versa - there are separate systems in place to handle those functions. Thus, having this information does not empower an attacker to impersonate a server/user or MITM a connection.

3.1.4 Debug Messages Enabled - FIXED

The ProtonVPN Windows 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

3.1.4.1 Recheck results

The following output is an excerpt of the debug messages produced by the application during the fix verification. OpenVPN/IKE2 usernames could not be identified from the log files:

```
2019-09-06 15:36:42.8580 INFO Trying to login user
2019-09-06 15:36:42.8580 INFO POST "/auth/info"
2019-09-06 15:36:43.0021 INFO POST "/auth/info": 200 OK
2019-09-06 15:36:43.2037 INFO POST "/auth"
2019-09-06 15:36:43.4557 INFO POST "/auth": 400 BadRequest
2019-09-06 15:36:43.4557 ERROR API: Request failed: Incorrect login
credentials. Please try again
2019-09-06 15:37:10.3039 INFO Trying to login user
2019-09-06 15:37:10.3039 INFO POST "/auth/info"
2019-09-06 15:37:10.4611 INFO POST "/auth/info": 200 OK
2019-09-06 15:37:10.6593 INFO POST "/auth"
2019-09-06 15:37:10.8751 INFO POST "/auth": 200 OK
2019-09-06 15:37:11.0763 INFO GET "/vpn"
2019-09-06 15:37:11.1818 INFO GET "/vpn": 200 OK
2019-09-06 15:37:13.5968 INFO GET "/vpn/logicals"
2019-09-06 15:37:13.7785 INFO GET "/vpn/logicals": 200 OK
2019-09-06 15:37:15.6564 INFO GET "/vpn/location"
2019-09-06 15:37:15.9005 INFO GET "/vpn/location": 200 OK
2019-09-06 15:37:15.9005 INFO GET "/vpn/clientconfig"
2019-09-06 15:37:16.0168 INFO GET "/vpn/clientconfig": 200 OK
2019-09-06 15:37:25.1686 INFO Sync profiles requested
```

3.1.5 OpenVPN UDP Listener on All Interfaces - FIXED

When a client connects to a VPN via UDP, the openvpn.exe creates a network process that listens on all network interfaces. An attacker that has network level access to the machine from which the VPN connection was initiated may be able to reach such listener. This may allow to misuse the legitimate OpenVPN tunnel or DoS the UDP listener to cause performance issues.

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:N/I:N/A:L

3.1.5.1 Recheck results

Like in the initial audit, when the VPN connection was initiated the following openvpn.exe process was created:

Process	CPU	Private Bytes	Working Set	PID	Description
ProtonVPNService.exe	0.09	43,384 K	62,248 K	5204	ProtonVPN
openvpn.exe		2,088 K	9,160 K	10028	
conhost.exe		6,416 K	10,744 K	3616	

Figure 2. openvpn.exe process (procexp64.exe output).

During the fix verification, however, no listeners tied to the above process ID were identified:

Process	PID	Protocol	Local Addr...	Local Port	Remote Address	Remote Port	State
openvpn.exe	10028	TCP	127.0.0.1	54346	0.0.0.0	0	LISTENING
openvpn.exe	10028	TCP	127.0.0.1	54346	127.0.0.1	15420	ESTABLISHED
openvpn.exe	10028	UDP	10.0.2.15	64204	*	*	
ProtonVPN.exe	7144	TCP	10.8.3.13	15434	104.18.42.158	80	ESTABLISHED
ProtonVPN.exe	7144	TCP	10.0.2.15	20773	185.70.40.230	443	ESTABLISHED
ProtonVPN.exe	7144	TCP	10.0.2.15	20776	185.70.40.230	443	CLOSE_WAIT
ProtonVPNService.exe	5204	TCP	127.0.0.1	15420	127.0.0.1	54346	ESTABLISHED

Figure 3. No tunnels listening on the IP address 0.0.0.0 (Tcpview.exe output).

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