SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Report 1907974

Source Code Review ProtonMail Bridge App

for

Proton Technologies AG

conducted by

SEC Consult

Version: 1.2 | **Date:** 2019-12-03
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 ProtonMail Bridge App for Windows – an application, which allows to send and receive encrypted emails in conjunction with any email client. 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:

- Is an attacker able to break end-to-end encryption provided by ProtonMail solution?
- Is an attacker able to access data of other customers (cross-tenant access)?

The initial review was conducted in Q1 2019 and a total effort of 5 days was dedicated to identifying and documenting security issues in the code base of the ProtonMail Bridge App.

Version 1.2.1 of the application was tested. Full access to the source code was granted.

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

Files	SHA1 Sum
Installers/Bridge-Installer.exe	f5f3d8e61b0c77b9b09bff550827c96787baf137
README.md	e5d9008d69f56ae507fbc89647c79637bc8fee8e
src_bridge_rc1.2.1_a755cf3.tgz	014eb44dea73a7cc4e134886a64009360b23bf88

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 one **low-risk vulnerability** in the reviewed source code and the app.

Although issues with certificate validation have been identified within the encrypted communication between the application and the backend system, the inner layer of end-to-end encryption could not be broken.

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 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	1	0
Medium	1	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
ProtonMail Bridge 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	ProtonMail Bridge App	Medium	ACCEPTED	6
Missing Certificate Pinning	ProtonMail Bridge App	Low	FIXED	8
Total	**-**	**Medium**	**-**	**-**

3 Detailed Analysis

This chapter outlines the attacks and found vulnerabilities in detail.

3.1 ProtonMail Bridge App

3.1.1 General Information

This section describes vulnerabilities found in the ProtonMail Bridge App.

The ProtonMail Bridge App provides paid desktop users a seamless email encryption and decryption through their favorite email client. During the timeframe of the review, the ProtonMail Bridge Windows app version 1.2.1 was tested on a fully patched Windows 10 x64 machine. The tested bridge app is written in Golang.

3.1.2 Sensitive Data in Memory - ACCEPTED

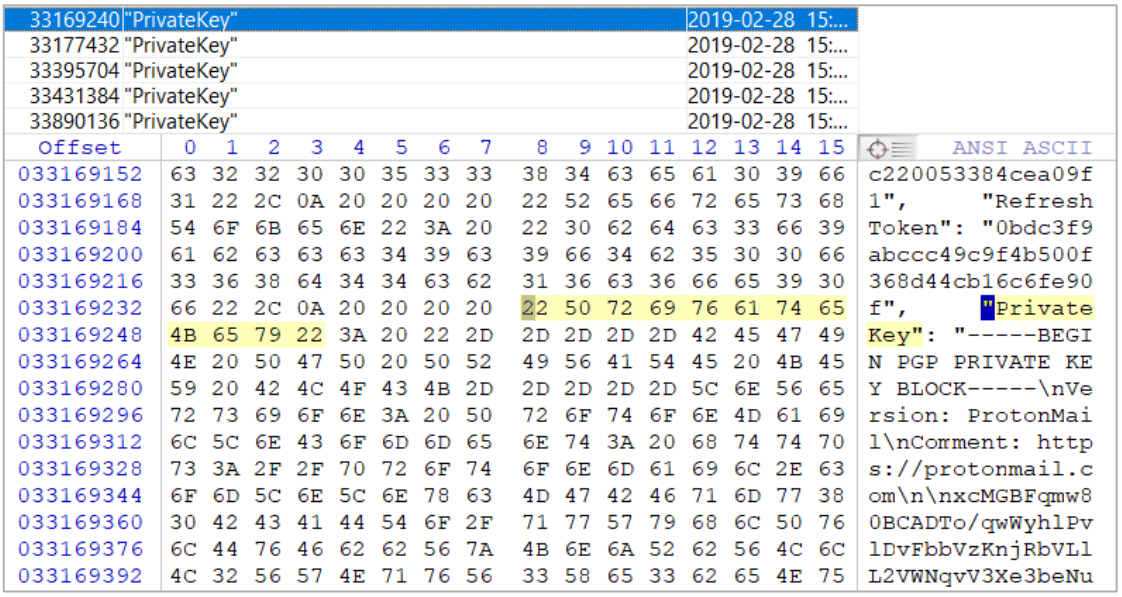
The tested Windows app temporarily stores data in memory for various processing purposes. The stored data includes plain text private PGP keys. If an attacker has access to the running bridge app process, he may be able to dump memory contents and identify sensitive information stored in it.

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 Desktop-Bridge.exe process was obtained. While analyzing the contents of the memory dump, a logged-in user's private PGP key (see figure below) and session tokens in plain text were identified.



```
33169240 "PrivateKey"                                   2019-02-28 15:...
33177432 "PrivateKey"                                   2019-02-28 15:...
33395704 "PrivateKey"                                   2019-02-28 15:...
33431384 "PrivateKey"                                   2019-02-28 15:...
33890136 "PrivateKey"                                   2019-02-28 15:...

Offset    0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15  ANSI ASCII
033169152 63 32 32 30 30 35 33 33  38 34 63 65 61 30 39 66  c220053384cea09f
033169168 31 22 2C 0A 20 20 20 20  22 52 65 66 72 65 73 68  1",     "Refresh
033169184 54 6F 6B 65 6E 22 3A 20  22 30 62 64 63 33 66 39  Token": "0bdc3f9
033169200 61 62 63 63 63 34 39 63  39 66 34 62 35 30 30 66  abccc49c9f4b500f
033169216 33 36 38 64 34 34 63 62  31 36 63 36 66 65 39 30  368d44cb16c6fe90
033169232 66 22 2C 0A 20 20 20 20  22 50 72 69 76 61 74 65  f",     "Private
033169248 4B 65 79 22 3A 20 22 2D  2D 2D 2D 2D 42 45 47 49  Key": "-----BEGI
033169264 4E 20 50 47 50 20 50 52  49 56 41 54 45 20 4B 45  N PGP PRIVATE KE
033169280 59 20 42 4C 4F 43 4B 2D  2D 2D 2D 2D 5C 6E 56 65  Y BLOCK-----\nVe
033169296 72 73 69 6F 6E 3A 20 50  72 6F 74 6F 6E 4D 61 69  rsion: ProtonMai
033169312 6C 5C 6E 43 6F 6D 6D 65  6E 74 3A 20 68 74 74 70  l\nComment: http
033169328 73 3A 2F 2F 70 72 6F 74  6F 6E 6D 61 69 6C 2E 63  s://protonmail.c
033169344 6F 6D 5C 6E 5C 6E 78 63  4D 47 42 46 71 6D 77 38  om\n\nxcMGBFqmw8
033169360 30 42 43 41 44 54 6F 2F  71 77 57 79 68 6C 50 76  0BCADTo/qwWyhlPv
033169376 6C 44 76 46 62 62 56 7A  4B 6E 6A 52 62 56 4C 6C  lDvFbbVzKnjRbVLl
033169392 4C 32 56 57 4E 71 76 56  33 58 65 33 62 65 4E 75  L2VWNqvV3Xe3beNu
```

Figure 1: Plain text private PGP key in memory.

The above memory dump was obtained after a user logged-out from the bridge app (after a logout the session tokens are invalidated, therefore the obtained plaintext session values would not create a risk), after the account was removed and after the cache and keychain was cleaned. Sensitive data in memory was only removed after the Desktop-Bridge.exe process was terminated.

Statement Proton Technologies AG:
Go garbage collector is outside of our control and there is no way to deterministically force it to clear unused memory; additionally, endpoint security is out of scope of the ProtonMail threat model, i.e. if an adversary can collect a memory dump of your machine, ProtonMail Bridge App will not save you; nevertheless, measures have been taken to try and reduce the number of instances of information in memory.

3.1.3 Missing Certificate Pinning - FIXED

Certificate Pinning allows 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

3.1.3.1 Recheck results

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

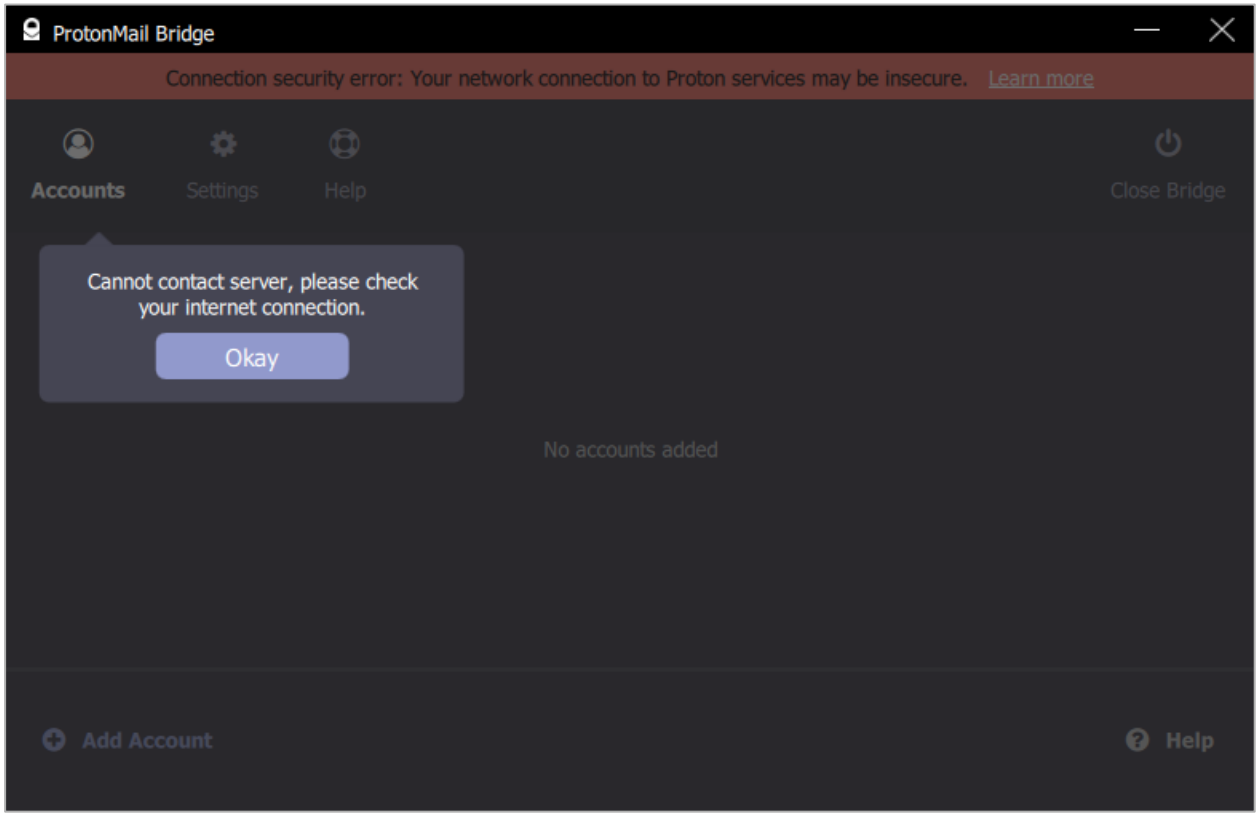


Figure 2. Certificate pinning is in place.

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	2019-12-03	Public report	SEC Consult	SEC Consult