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

Table of Contents ................................................................................................................. 2  
1 Management Summary ...................................................................................................... 3  
  1.1 Scope and Timetable ....................................................................................................... 3  
  1.2 Results .......................................................................................................................... 4  
  1.3 Disclaimer ..................................................................................................................... 4  
2 Vulnerability Summary ...................................................................................................... 5  
  2.1 Total Risk Per System ..................................................................................................... 5  
  2.2 Risk of Each Vulnerability ............................................................................................ 5  
3 Detailed Analysis ................................................................................................................ 6  
  3.1 ProtonMail Bridge App .................................................................................................. 6  
    3.1.1 General Information .................................................................................................. 6  
    3.1.2 Sensitive Data in Memory - ACCEPTED ................................................................. 6  
    3.1.3 Missing Certificate Pinning - FIXED ....................................................................... 8  
4 Version History .................................................................................................................. 9
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:

<table>
<thead>
<tr>
<th>Files</th>
<th>SHA1 Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installers/Bridge-Installer.exe</td>
<td>f5f3d8e61b0c77b9b09bff550827c96787ba137</td>
</tr>
<tr>
<td>README.md</td>
<td>e5d9008d69f56ae507fbc89647c79637bc8fee8e</td>
</tr>
<tr>
<td>src_bridge_rc1.2.1_a755cf3.tgz</td>
<td>014eb44dea73a7cc4e134886a64009360b23bf88</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Risk assessment</th>
<th>Initial no. of vulnerability classes</th>
<th>Current no. of vulnerability classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Medium</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Critical</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

2.1 Total Risk Per System
The following table contains a risk assessment for each system which contained security flaws.

<table>
<thead>
<tr>
<th>System</th>
<th>Field of application</th>
<th>Initial risk</th>
<th>Current risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProtonMail Bridge App</td>
<td>Desktop</td>
<td>Medium</td>
<td>-</td>
</tr>
<tr>
<td>Total</td>
<td>-</td>
<td>Medium</td>
<td>-</td>
</tr>
</tbody>
</table>

2.2 Risk of Each Vulnerability
The following table contains a risk assessment for the discovered vulnerabilities.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>System</th>
<th>Initial risk</th>
<th>Current risk</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive Data in Memory</td>
<td>ProtonMail Bridge App</td>
<td>Medium</td>
<td>ACCEPTED</td>
<td>6</td>
</tr>
<tr>
<td>Missing Certificate Pinning</td>
<td>ProtonMail Bridge App</td>
<td>Low</td>
<td>FIXED</td>
<td>8</td>
</tr>
<tr>
<td>Total</td>
<td>-</td>
<td>Medium</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
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)


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.
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:

![Certificate pinning is in place.](image-url)

*Figure 2. Certificate pinning is in place.*
## 4 Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Status/Changes</th>
<th>Created by</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2019-03-15</td>
<td>Initial report</td>
<td>SEC Consult</td>
<td>SEC Consult</td>
</tr>
<tr>
<td>1.1</td>
<td>2019-10-10</td>
<td>Fix verification</td>
<td>SEC Consult</td>
<td>SEC Consult</td>
</tr>
<tr>
<td>1.2</td>
<td>2019-12-03</td>
<td>Public report</td>
<td>SEC Consult</td>
<td>SEC Consult</td>
</tr>
</tbody>
</table>