securITum

Security report

SUBJECT

Security audit of Proton Drive application for iOS platform

DATE

23.08.2022 – 06.09.2022

RETEST DATE

N/A

LOCATION

Cracow (Poland)

AUDITORS

Artur Czyż

VERSION

1.0

Executive summary

This document is a summary of work conducted by Securitum company. The subject of the test was the Proton Drive mobile application for iOS platform (without API/backend), and automatic analysis of the application's source code.

Tests were conducted using the role of unlogged and logged in user.

During the tests, particular emphasis was placed on vulnerabilities that might in a negative way affect confidentiality, integrity or availability of processed data.

The security tests were carried out in accordance with generally accepted methodologies, including: OWASP TOP10, (in a selected range) OWASP MASVS, OWASP ASVS as well as internal good practices of conducting security tests developed by Securitum.

An approach based on manual tests (using the above-mentioned methodologies), supported by a number of automatic tools (i.a. Burp Suite Professional, ffuf, Objection, Frida, MobSF, Drozer, SonarQube), was used during the assessment.

During the automatic analysis of the application's source code, no security vulnerabilities were identified.

The vulnerabilities are described in detail in further parts of the report.

Risk classification

Vulnerabilities are classified in a five-point scale, that is reflecting both the probability of exploitation of the vulnerability and the business risk of its exploitation. Below, there is a short description of meaning of each of severity levels:

- CRITICAL – exploitation of the vulnerability makes it possible to compromise the server or network device, or makes it possible to access (in read and/or write mode) data with a high degree of confidentiality and significance. The exploitation is usually straightforward, i.e. an attacker does not need to gain access to the systems that are difficult to reach and does not need to perform any kind of social engineering. Vulnerabilities marked as 'CRITICAL' must be fixed without delay, especially if they occur in production environment.

- HIGH – exploitation of the vulnerability makes it possible to access sensitive data (similar to 'CRITICAL' level), however the prerequisites for the attack (e.g. possession of a user account in an internal system) makes it slightly less likely. Alternatively, the vulnerability is easy to exploit, but the effects are somehow limited.

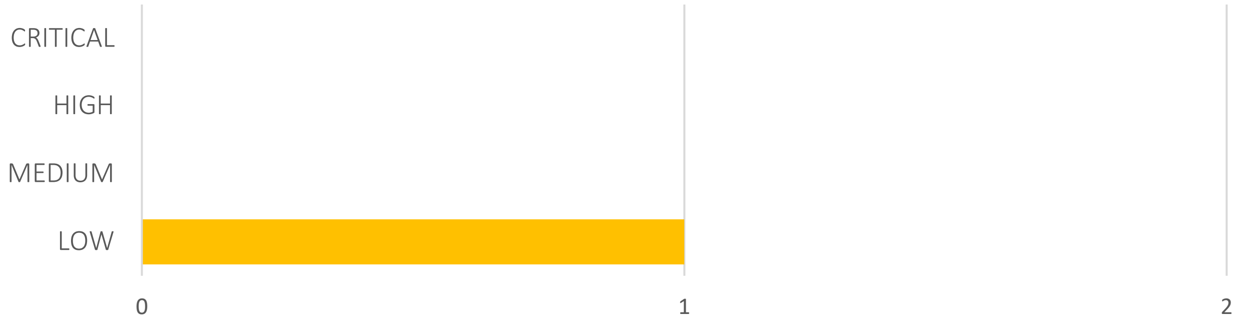
- MEDIUM – exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.

- **LOW** – exploitation of the vulnerability results in minor direct impact on the security of the test subject or depends on conditions that are very difficult to achieve in practical manner (e.g. physical access to the server).

- **INFO** – issues marked as ‘INFO’ are not security vulnerabilities per se. Their aim is to point out good practices, the implementation of which will lead to the overall increase of the system security level. Alternatively, the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.

Statistical overview

Below, a statistical overview of vulnerabilities is shown:



Additionally, 4 INFO issues are reported.

Contents

Change history

Document date	Version	Change description
07.09.2022	1.0	Final version.

Vulnerabilities in the mobile application

[LOW] SECURITUM-226099-001: Insecure mechanism for storing confidential information

Summary

It was found that application stores the cookies and HTTP responses in unencrypted application files. This data in case of physical access to the device could allow an attacker to gather sensitive data such as cookies.

More information:

- https://cwe.mitre.org/data/definitions/522.html
- https://cwe.mitre.org/data/definitions/312.html

Prerequisites for the attack

Physical access to the device.

Technical details (proof of concept)

`/var/mobile/Containers/Data/Application/CDFB6763-5BC2-4981-9DC5-B8ED4C837B2A/Library/Cookies/Cookies.binarycookies` file contains the following sensitive data:

```
Name
Domain
Path
Secure
HTTPOnly
Value
SessionOnly
SameSitePolicy
Session-Id     ec2-[...]45.eu-central-1.compute.amazonaws.com     /
Yx[…]YE
Session-Id     ec2-[...]157.eu-central-1.compute.amazonaws.com    /
Yx[…]YE
Session-Id     .protonmail.ch /
Yx[…]YE
```

In the folder: `/var/mobile/Containers/Data/Application/CDFB6763-5BC2-4981-9DC5-B8ED4C837B2A/Library/Caches/ch.protonmail.drive/Cache.db-wal`, cached HTTP responses, containing session cookie may be found (highlighted in yellow, in the below dump):

```
__CFURLStringType\_CFURLString_yhttps://[...]aqjx[...]ep.dm[...]a.protonpro.xyz#@4___CFURLRequest
NullTokenString__     [...]SGET[...]VAccept_Accept-Language_Accept-EncodingX__hhaa__S*/*Upl-
pl_gzip, deflate, br_[...]
[...]
YnBs[...]A67<O\^
[...]<{"Status":0,"TC":false,"RD":true,"RA":true,"AD":false,"CD":false,"Question":[{"name":"a[...
]ua.protonpro.xyz.","type":16}],"Answer":[{"name":"aq[...]ua.protonpro.xyz.","type":5,"TTL":120,"
data":"dm[...]ua.protonpro.xyz."},{"name":"dm[...]ua.protonpro.xyz.","type":16,"TTL":120,"data":"
ec2-[...]7.eu-central-
1.compute.amazonaws.com"},{"name":"dm[...]ua.protonpro.xyz.","type":16,"TTL":120,"data":"ec2[...]
45.eu-central-1.compute.amazonaws.com"}],"Comment":"Response from 17[...]8."}  E:[...]
```

Location

Multiple folders located in `/var/mobile/Containers/Data/Application/CDFB6763-5BC2-4981-9DC5-B8ED4C837B2A/Library/Caches/` directory.

Recommendation

Sensitive data should not be stored in the mobile device file system. This kind of data should be stored only on the server-side (If it is necessary to store sensitive data in the mobile device file system, it should be encrypted). When there is a need to process data, it should be downloaded and processed only in the device memory.

Encryption key should be generated on the mobile device and stored on the server in an encrypted form (key to decrypt data key should be stored in the keystore). Access to the encryption key must require successful login attempt.

Recommendations related to the mobile application

[INFO] SECURITUM-226099-002: Lack of information about the use of a dangerous device

SUMMARY

The application does not inform a user about the risks associated with running the application on a dangerous - jailbroken device.

Applications installed on a jailbroken phone have a much wider scope of reading or modifying critical data, such as authorization data. Users with jailbroken devices are more vulnerable to attacks than those who use non-jailbroken devices.

This is not a description of vulnerability, but a recommendation, of which implementation may increase the overall level of system security.

LOCATION

Proton Drive application for iOS platform.

RECOMMENDATION

It is recommended to implement a mechanism which task will be to verify if the device on which the tested application is installed has been previously jailbroken. If the device is confirmed as jailbroken, it is recommended to take appropriate measures, for example:

- displaying a warning message with information about the use of a dangerous device,
- logging information about starting the application on a dangerous device,
- blocking the ability to run applications on a dangerous device.

It is worth considering the implementation of a very strict rule, i.e. the user should not be able to run the application on a jailbroken device.

In case of implementing restrictive policies, such as the inability to run applications on a dangerous device, it is recommended to provide two versions of the application for testing – one in which this mechanism is active and the other without it enabled.

[INFO] SECURITUM-226099-003: Lack of obligation to use the minimum security to protect access to the device

SUMMARY

It is a good practice, to convince the user to use the device access security (such as screen lock code). An attacker who gains access to the user's device will be able to run the user’s application and act on his or her behalf.

This is not a description of vulnerability, but a recommendation, of which implementation may increase the overall level of system security.

LOCATION

Proton Drive application for iOS platform.

RECOMMENDATION

The application should force the user to use the access code (e.g. PIN, password) on the mobile device. This will increase the level of security of mobile devices on which the mobile application will be installed. Modern mobile operating systems have data encryption enabled when the phone is locked.

[INFO] SECURITUM-226099-004: Lack of security for access to the application

SUMMARY

The audit of the application has shown that it does not implement any additional authentication layer after a user first authenticates in the application. After the application is restarted it does not require the user to authenticate again before giving the access to its content. Such a solution may expose the user to a data leak, e.g. in the case when a mobile device is stolen.

This is not a description of vulnerability, but a recommendation, of which implementation may increase the overall level of system security.

LOCATION

Proton Drive application for iOS platform.

RECOMMENDATION

It is recommended to implement a mechanism that will force the user to enter, for example, a PIN before it is allowed to access the application resources. It should be noted that the verification of the PIN should take place on the server side.

[INFO] SECURITUM-226099-005: Lack of application integrity checking and modification protection

Summary

The tested application does not have any security features or mechanisms to prevent it from being injected with various types of scripts, i.e. Frida Gadgets. An attacker using this fact can add malicious code to the application to better understand its operation.

This is not a description of vulnerability, but a recommendation, of which implementation may increase the overall level of system security.

Location

Proton Drive application for iOS platform.

Recommendation

It is recommended to implement security features or mechanism that will protect the application from being injected with various types of scripts, i.e. Frida Gadgets.