securitum

Security report

SUBJECT

Security audit of Proton Drive application for Android platform

DATE

29.07.2022 – 22.08.2022

RETEST DATE

N/A

LOCATION

Cracow (Poland)

AUDITORS

Marek Rzepecki

VERSION

1.0

securitum

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 Android platform, its REST API, and automatic tests 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.

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.

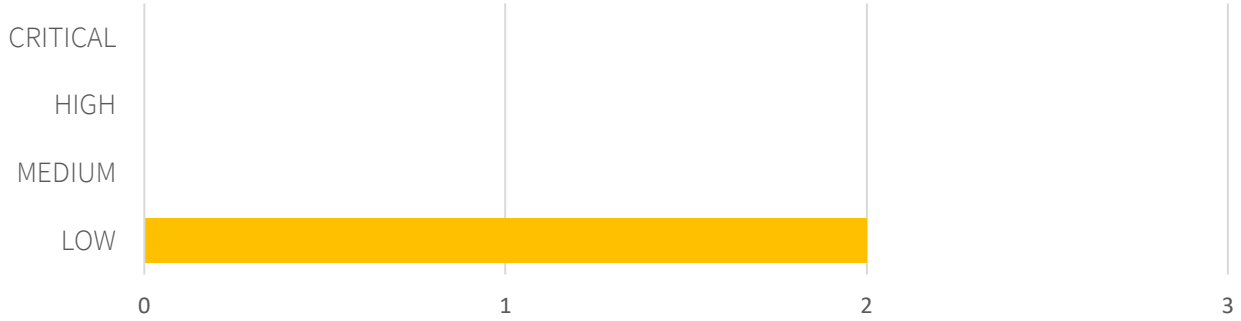
- HIGH – exploitation of the vulnerability makes it possible to access sensitive data (similar to 'CRITICAL' level), however the prerequisites for the attack (e.g. possession of a user account in an internal system) makes it slightly less likely. Alternatively, the vulnerability is easy to exploit, but 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, 6 INFO issues are reported.

Contents

Change history

Document date	Version	Change description
22.08.2022	1.0	Final version.

Vulnerabilities in the mobile application

[LOW] SECURITUM-226093-001: Insecure mechanism for storing confidential information

SUMMARY

It was found that application stores the cookies, HTTP responses, public and private certificates, in the application files, in an unencrypted form. This data, in case of physical access to the device, could allow an attacker to gather sensitive data, such as cookies, and keys used in the encryption process.

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)

`/data/user/0/me.proton.android.drive/files/datastore/protonCookieStore` file contains the following sensitive data:

```
me.proton.android.drive on (google: 10) [usb] # file cat protonCookieStore
Downloading /data/user/0/me.proton.android.drive/files/datastore/protonCookieStore
[…]
====
{"map":{"name=Tag domain=fra-storage.proton.me
path=/":{"name":"Tag","value":"default","expiresAt":1668940003888,"domain":"fra-
storage.proton.me","hostOnly":true,"path":"/","secure":true,"httpOnly":false},"name=Session-Id
domain=protonmail.com path=/":{"name":"Session-
Id","value":"[…]AAPM","expiresAt":1668940396278,"domain":"protonmail.com","hostOnly":false,"path"
:"/","secure":true,"httpOnly":true},"name=Tag domain=drive.protonmail.com
path=/":{"name":"Tag","value":"redirect","expiresAt":1668940396279,"domain":"drive.protonmail.com
","hostOnly":true,"path":"/","secure":true,"httpOnly":false}}}====
Personal data is also located in SQLite databases:
```

In the folder: `/data/user/0/me.proton.android.drive/cache/http_cache/`, cached HTTP responses, containing session cookie and certificates, may be found (cookie and key was highlighted in yellow, in the below dump):

```
me.proton.android.drive on (google: 10) [usb] # file cat f5ca4e80dce8afcc5ed24b6541943f82.0
Downloading
/data/user/0/me.proton.android.drive/cache/http_cache/f5ca4e80dce8afcc5ed24b6541943f82.0 [...
[…]
====
https://drive.protonmail.com/api/drive/shares/@3cvhu8PZRO4NLoEDzOF5U_Afd1b9ViTBRPY8uX4Tr7cSzIt07T
4dFJ0mqcs0BNwE-As4fCP-
lMFUvHHv3SVELg==/files/@PtOsEc5em9FZHMnaOddpdAHKf8Z7EOV0zcWEnBzmTIYqdJUJ5_qpgtnbDJ-
UbblWEFAEBHl02DXFLKqIoyhLiw==/revisions/@btVrzZqS_qH1lFNWEn3yMC5KFMjv50MUvYrdAv1zCChh5nHmlue6TZ1y
vjjLlt_a7AVM1qoSdEtqE6a-cdxpsw==?FromBlockIndex=1&PageSize=150
GET
1
Accept-Encoding: gzip
```

```
HTTP/1.1 200
21
date: Mon, 22 Aug 2022 10:26:49 GMT
expires: Mon, 22 Aug 2022 10:50:50 GMT
cache-control: immutable, private
access: application/vnd.protonmail.api+json;apiversion=3
vary: Accept-Encoding
set-cookie: Session-Id=YwN[…]; Domain=protonmail.com; Path=/; HttpOnly; Secure; Max-Age=7776000
set-cookie: Tag=redirect; Path=/; Secure; Max-Age=7776000
[…]

TLS_AES_256_GCM_SHA384
2
MIIDpTCCAo2gAwIBAgIEOvp[…]/JuNupKL/zlB1HUpN1xvPRxtI6t+SW0bWkfLa
0
TLSv1.3
```

The folders: `/data/user/0/me.proton.android.drive/no_backup/`, `/data/user/0/me.proton.android.drive/databases/` contains unencrypted application databases, with user-related data. View of the `db-drive` database:

```
sqlite> .tables
AccountEntity               NotificationEventEntity
AccountMetadataEntity       OrganizationEntity
AddressEntity               OrganizationKeysEntity
AddressKeyEntity            PublicAddressEntity
ChallengeFrameEntity        PublicAddressKeyEntity
DownloadBlockEntity         SessionDetailsEntity
DriveLinkRemoteKeyEntity    SessionEntity
EventMetadataEntity         ShareEntity
FeatureFlagEntity           ShareUrlEntity
FolderMetadataEntity        SortingEntity
HumanVerificationEntity     TrashMetadataEntity
KeySaltEntity               TrashWorkEntity
LinkDownloadStateEntity     UiSettingsEntity
LinkEntity                  UploadBlockEntity
LinkFilePropertiesEntity    UserEntity
LinkFolderPropertiesEntity  UserKeyEntity
LinkOfflineEntity           UserSettingsEntity
LinkTrashStateEntity        VolumeEntity
LinkUploadEntity            android_metadata
MessageEntity               room_master_table
NotificationChannelEntity
sqlite> select * from UserKeyEntity;
PI0cbT_-qHACInfBE24mxjrD-MUN9iOJoo8FWYE8BG2INhFzQgI90khpahaEoYJAtGadZSBs7xUYYA5e8KNNJg=
LOCK-----
Version: ProtonMail

xYYEYtZsChYJKwYBBAHaRw8BAQdAwUiwTEB49PUUhcUpk10Yyn3ETztZ14kM
h/QNY/yMTar+CQMIX7MLBWv9q6dg6Y2Cp907lEsNVmdclAjpPQQsVOKmkmdx
[redacted]
bAoCGwwAIQkQ5Ovg7q/1BiUWIQQZtGR9LnWpvgO+1Zrk6+Dur/UGJWXHAP9A
UckFPZInrJzGdgf4kV6iBs5gIWroRsSTAzmcrbF9owEAweP/11eJBQhh5y9K
izTigsYOcDa2PqEZvQIjzD/xjAc=
=EEdj
-----END PGP PRIVATE KEY BLOCK-----
|1|1|||1
sqlite>
```

LOCATION

Multiple folders located in `/data/user/0/me.proton.android.drive/` 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-226093-002: 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 – rooted – device.

Applications installed on a rooted phone have a much wider scope of reading or modifying critical data, such as authorization data. Users with rooted devices are more vulnerable to attacks than those who use non-rooted 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 Android 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 rooted. If the device is confirmed as rooted, 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 rooted 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-226093-003: Lack of masking of application screens while minimizing the application

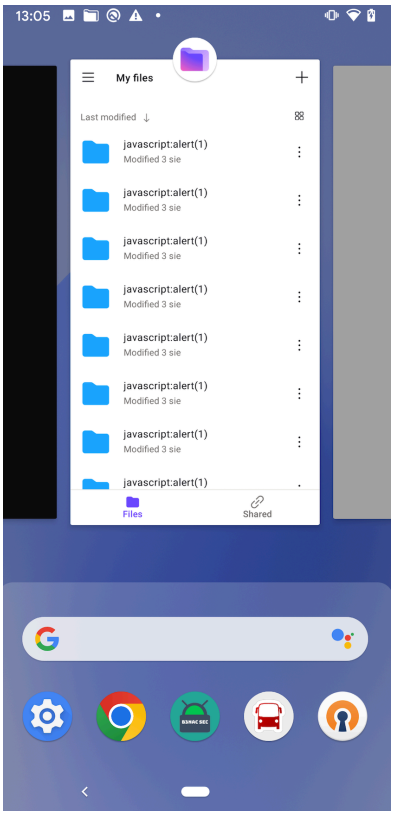
SUMMARY

The tested application processes sensitive data, such as files uploaded by a user. When the user minimizes the application on the login screen, the device will take a screenshot of the application and save it on the device (in thumbnail file). Due to that, it exposes the user to the risk of the sensitive information getting leaked.

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

TECHNICAL DETAILS (PROOF OF CONCEPT)

Auto-generated screenshot containing personal data:



LOCATION

Proton Drive application for Android platform.

RECOMMENDATION

It is recommended to change the graphics showed in the application miniatures (e.g. for the company logo).

More information:

- https://developer.android.com/reference/android/view/WindowManager.LayoutParams.html#FLAG_SECURE

[INFO] SECURITUM-226093-004: 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 Android 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-226093-005: 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 Android 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-226093-006: 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 Android 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.

Vulnerabilities in the API

[LOW] SECURITUM-226093-API-001: Incorrect CORS configuration

SUMMARY

The analysis showed that the API does not have a correct validation of the `Origin` header, which is sent in each request. At the moment, it is possible to enter any value into this header, which then will be accepted by the server.

As a consequence, an attacker may potentially be able to circumvent the Same-Origin Policy (SOP) mechanism and perform a number of malicious actions such as stealing cookies, sending own HTTP requests or compromising confidential information of other users (if other vulnerabilities are detected).

More information:

- https://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny

PREREQUISITES FOR THE ATTACK

None.

TECHNICAL DETAILS (PROOF OF CONCEPT)

Example of the HTTP request sent to the application:

```
PUT /api/settings/flags HTTP/2
Host: drive.proton.me
Cookie: […]
User-Agent: Mozilla[…]
Accept: application/vnd.protonmail.v1+json
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 14
X-Pm-Appversion: web-drive@5.0.4.5
X-Pm-Uid: 2gb2r3xqhryqef3vvkwuw2opuf7impsm
Origin: https://sbqkbckndrive.proton.me
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer:
https://drive.proton.me/u/0/%3fgdr%26rrb%3d1/drive/shares/@3cvhu8PZRO4NLoEDzOF5U_Afd1b9ViTBRPY8uX
4Tr7cSzIt07T4dFJ0mqcs0BNwE-As4fCP-
lMFUvHHv3SVELg==/folders/@X64p9tXaTTTRMacUEhraqI4VIrDcDY8JMFnhed7u9lILiA8CKVFDPfOaQnByO7L8dbm64Ty
zOtAMHnqh3Z75JQ==/children?Page=0&PageSize
Te: trailers

{"Welcomed":1}
```

In response, the API returns:

```
HTTP/2 200 OK
Date: Wed, 03 Aug 2022 13:10:22 GMT
Cache-Control: max-age=0, must-revalidate, no-cache, no-store, private
Expires: Fri, 04 May 1984 22:15:00 GMT
Access: application/vnd.protonmail.api+json;apiversion=3
Access-Control-Allow-Origin: https://sbqkbckndrive.proton.me
```

```
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Date, Retry-After
[…]

{"Code":1000}
```

LOCATION

https://drive.proton.me

RECOMMENDATION

It is recommended to set a fixed value for the `Access-Control-Allow-Origin` header (and `Origin`) or to accept only trusted domains (whitelist).

More information:

- https://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny
- https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html
- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Recommendations related to the API

[INFO] SECURITUM-226093-API-002: X-XSS-Protection header enabled

SUMMARY

It was observed that HTTP responses contain `X-XSS-Protection` header. This header is not supported anymore by majority of the browsers (such as Chrome, Mozilla Firefox, Microsoft Edge), and in very rare and specific cases may open an application to the XS-Leak vulnerability. The role of `X-XSS-Protection` header was taken over by a Content Security Policy.

More information:

- https://markitzeroday.com/headers/content-security-policy/2018/02/10/x-xss-protection.html
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://portswigger.net/daily-swig/google-deprecates-xss-auditor-for-chrome

More information on XS-Leak attack:

- https://owasp.org/www-pdf-archive/AppSecIL2015_Cross-Site-Search-Attacks_HemiLeibowitz.pdf

LOCATION

https://drive.protonmail.com

RECOMMENDATION

It is recommended to verify if the `X-XSS-Protection` header is necessary (for example, if an application is used in very old browsers, which do not support Content Security Policy). If not, it should be deleted.

It should be noted that its occurrence does not automatically open an application to new vulnerabilities (as the exploitation of XS-Leaks may be very sophisticated and not possible in each case), and this recommendation is only a suggestion, allowing for additional hardening.