wandera

THREAT ADVISORY

SkyDemon mobile apps & website

SEVERITY	TYPE	IMPACT	TARGET	REPONSE
3/5	CREDENTIALS	HIGH	ANDROID, IOS	IMMEDIATE

SUMMARY

SkyDemon is one of Europe's most popular solutions for VFR flight planning and in-flight navigation.

The mobile apps allow a user to access their SkyDemon subscription on an Android or iOS device, unlocking SkyDemon's powerful features while on the move.

Harnessing the power of MI:RIAM, the Wandera team has detected that the communication of the mobile application with the backend is accomplished in plain-text, and that the only protected parameter is the password. This protection is in place during the login procedure. The password is hashed with the SHA1 algorithm, then base64 encoded.

Unfortunately this constitutes a poor means of protection, although the plain-text password is not revealed. The login procedure is susceptible to a "pass the hash" attack. This type of attack is a hacking technique that allows an agent to authenticate to a remote service just by using the underlying hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

SECURITY IMPLICATIONS

SkyDemon apps usually are popular among student and trainee pilots, as well as with hobbyist pilots for small aircraft. Although the use-case is seemingly limited to a niche audience, with up to 50,000 downloads SkyDemon has a significant market penetration - with plenty more making use of the SkyDemon website too.

If the SkyDemon app becomes compromised, a hacker could use the exposed information to track and spy on users.

This data could lead to other sensitive information being leaked, such as flight plans, aircraft model registration details and even behavioural patterns like favourite destinations. All the flight related information simply comes on top of the already exposed personal information.

The following personally identifiable information (PII) is exposed during the login procedure on the mobile application:

- Username
- Base64 encoded SHA1 Password

The following PII is exposed during the "Password Reset" functionality on the mobile application:

- Email

ABOUT SKYDEMON

What:
An app and web service for flight planning and navigation

Global impact:
everyone using the applicationt

Installations:
10,000 - 50,000

Android App:
https://play.google.com/store/apps/details?id=aero.skydemon.skydemonandroid

iOS App:
https://itunes.apple.com/gb/app/skydemon/id497184081?mt=8

Action required:
Implement TLS encryption

The following PII is exposed when a user requests for a free trial through the website:

- E-mail
- First, Last Name
- Country

REMEDIATION AND PREVENTION

SkyDemon should employ encryption throughout the all communications across both the website and mobile application with the back-end service.

Our recommendation is for businesses to have an active mobile security service deployed. MDMs are able to restrict access to certain apps, but are unable to limit access to websites. These technologies should have filtering and blocking functionality that happens at the data level to block traffic to both leaky apps and vulnerable websites.

We have included some examples of exposed information.

Example of a user login request via the Android app

```
“POST /data/loginuser.aspx?login=makis%40makis.gr&password=T%2FGjPhiLe4YSPW474nI–
qI1FKg7Q%3D&device=A%7Cb48da99360645e89&devicetype=samsung%7CSM–A300FU&ver–
sion=3.6.3.28529&random=294923100 HTTP/1.1
Content–Length: 1
Expect: 100–continue
Host: data.skydemon.aero
Connection: close”
```

Example of the password reset functionality via the Android app

```
“POST /members/forgotpassword.aspx?action=reset&email=xxx@xxx.xxx&random=xxxxxx
HTTP/1.1
Content–Length: 1
Expect: 100–continue
Host: www.skydemon.aero
Connection: close”
```

Example of a user login request via the iOS app

```
“POST /data/loginuser.aspx?login=xxxx@xxxxx.xxx&password=xxxxxxxxx&de–
vice=I%xxxxxxxxxxxxxxxxxxxxx&devicetype=xxxxxx&version=xxxxxx&random=xxxxxxx
HTTP/1.1
Content–Length: 1
Expect: 100–continue
Host: data.skydemon.aero
Connection: close”
```

Example of the password reset functionality via the the iOS app

```
“POST /members/forgotpassword.aspx?action=reset&email=xxxxx@xxxx.xxx&random=xxxxxxx
HTTP/1.1
Content–Length: 1
Expect: 100–continue
Host: www.skydemon.aero
Connection: close”
```

ABOUT MI:RIAM

Part of our mission at Wandera is to conduct threat research and rapid identification for the purpose of advancing customers' mission-critical security operations and defending their mobile device and data assets from attack.

The engine at the heart of our intelligence is called MI:RIAM. Using a sophisticated blend of machine learning and artificial intelligence, MI:RIAM has been created to detect new threats and vulnerabilities, exposing previously hidden information on actors, attacks, breaches and signatures.

Wandera is the leader in mobile data security and management, providing enterprises with unrivaled visibility into their mobile data, and protecting them with real-time threat prevention, compliance and data cost management.

Learn more at *wandera.com*