wandera

THREAT ADVISORY

Bluclub

SEVERITY	TYPE	IMPACT	TARGET	REPONSE
5/5	PII LEAK, CREDIT CARD LEAK	HIGH	APP	IMMEDIATE

SUMMARY

Wandera's threat detection team, using the powerful machine learning capabilities of MI:RIAM, has discovered a severe vulnerability in a mobile application called "Bluclub" that put personally identifiable information (PII) and users' credit card information at risk. These data leaks are a result of a lack of security in data transit by the application.

Bluclub is a relatively new car service, based in Brazil, featuring a 100% armoured vehicle fleet and drivers that are trained in defensive driving. It positions itself as valuing the comfort, safety and protection of its occupants above all else. Ironically, the security it offers within its vehicles doesn't translate to the mobile application.

SECURITY IMPLICATIONS

Both the iOS and Android versions of the application are using HTTP protocol in order to transmit sensitive user information. This means that personal credentials including username, password, name and phone number are transferred completely unencrypted, and therefore unprotected over-the-air during the app's login and registration processes. The lack of HTTPS protocol makes the data essentially defenceless to third party attacks.

Due to the commercial nature of the application, credit card information must also be shared with the company. This includes full credit card numbers as well as expiry dates - everything a malicious attacker would be looking for. Again, this data travels over the internet in plaintext due to the HTTP protocol, enabling hackers to easily access the information with the right tools.

The implications of this threat are deeply concerning for the users of Bluclub. Access to personal information (including credit card details) makes identity theft an easy feat for the average hacker. The conflicting nature of a car service centered around security for its customers, while at the same time leaking their personal and credit card information is troubling.

RISK DETAILS

Wandera researchers have discovered data leaks occurring during the login and registration request processes in both the Android and iOS versions of the application. This results in the following sensitive PII and credit card information being exposed:

PII that is exposed when a user registers the app and creates an account includes:

- Username
- Password
- First and Last name
- E-mail
- Phone Number
- Password
- Credit Card Details (number, type, expiration date)

ABOUT THE BLUCLUB THREAT

What:
The "Bluecub" app

Global impact:
Everyone using the application.

Installations:
5,000 - 10,000

Android App:
https://play.google.com/store/apps/details?id=br.com.bluclub

iOS App:
https://itunes.apple.com/br/app/bluclub/id1170631460?mt=8

Action required:
Disable the HTTP protocol and adopt only HTTPS.

REMEDIATION AND PREVENTION

Both businesses and users should have an active mobile security service deployed to block data leaks among applications used. They should also avoid using risky or unknown applications over public and potentially insecure WiFi hotspots in order to minimize the risk of traffic interception.

A content filtering service is also recommended to restrict access to newly-identified risky domains and services as soon as they emerge, such as this one.

The developers of the BluClub app are advised to utilize SSL/TLS in order to protect the transmission of personally identifiable user information, session tokens, or other sensitive data to a backend API or web service.