## THREAT ADVISORY

# Bookairfare.com

| SEVERITY | TYPE | IMPACT | TARGET | REPONSE |
|----------|------|--------|--------|---------|
| 3/5 | PII LEAK, CREDIT CARD LEAK | HIGH | WEBSITE | IMMEDIATE |

## SUMMARY

Wandera researchers have discovered a data leak in the mobile microsite of a travel website called bookairfare.com (m.bookairfare.com). This is due to the transfer of personally identifiable information (PII) and credit card details unencrypted over-the-air.

In operation since 2006, bookairfare.com is a travel website that enables customers to book flights, hotels and cars for their trips. The site is quite popular in North America, particularly in the US. Bookairfare.com positions itself as the first completely independent flight booking engine, presenting users with the lowest possible travel prices upfront.

## SECURITY IMPLICATIONS

The primary vulnerability in the mobile website has been identified by MI:RIAM as the transmission of customer PII and credit card information over the insecure and unencrypted HTTP channel during the booking request.

This means the user's information travels over the internet in plaintext, making its exposure to third parties very likely

The data leak, however, is happening only on the mobile site. If the website is visited from a laptop or desktop, users' information remains secure as it is transferred over the encrypted HTTPS channel.

## RISK DETAILS

The PII exposed during the booking request on the mobile site includes:

*Name, Surname Credit Card Number, Credit Card Expiry Dates, Credit Card Security Code, Billing Address Details, City, Zip/Postal Code, Country, State*

## REMEDIATION AND PREVENTION

Users should have an active mobile security service deployed to monitor and block data leaks. They should also avoid using the website over public and potentially insecure Wi-Fi hotspots in order to minimize the risk of traffic interception.

The developers of the bookairfare.com 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.

### BookAirfare

**ABOUT THE BOOKAIRFARE.COM THREAT**

**What:**
Travel website that enables the booking of flights, hotels and cars

**Global impact:**
Everyone using the mobile website

**Action required:**
disable the HTTP protocol and adopt only HTTPs (enable encryption)