wandera

THREAT ADVISORY

Ticketac mobile apps

SEVERITY	TYPE	IMPACT	TARGET	REPONSE
5/5	CREDIT CARD LEAK, CREDENTIALS LEAK, CROSS-SITE SCRIPTING	HIGH	ANDROID, IOS	IMMEDIATE

SUMMARY

Researchers at Wandera have identified a vulnerability in the official mobile apps from Ticketac that puts personally identifiable information (PII) at risk. Specifically, the mobile apps fail to use encryption to protect sensitive information, such as email, password and credit card details, when it is sent across the Internet.

Ticketac is a popular web service through which one can book theater tickets, shows, concerts and one-man-shows at reduced prices throughout France.

SECURITY IMPLICATIONS

The vulnerability identified by Wandera impacts both the Android and iOS mobile apps from Ticketac. Specifically, both the login and initial account creation processes fail to protect personal information. This results in user credentials being transmitted without any encryption at all, exposing it to any attacker or third party observer on the network.

Additionally, Wandera's researchers have observed that credit card related details are transmitted over an insecure connection during the booking process.

Finally, although the website is using an encrypted connection and is not susceptible to the aforementioned attacks, it is vulnerable to reflected cross-site scripting attack vector which in effect can be used to hijack a user's session, if combined with a successful social engineering campaign.

CROSS SITE SCRIPTING

XSS attacks allow the attacker to compromise a user's session by using malicious code running at the client-side. For example: if an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

Since cookies are used as a session management mechanism, it's possible for an attacker to create a specific JavaScript code that will send the cookie back to him. As a result the attacker can gain unauthorized access to the user's personal account and impersonate the user.

ABOUT THE TICKETAC THREAT

What:
Ticket purchasing web service

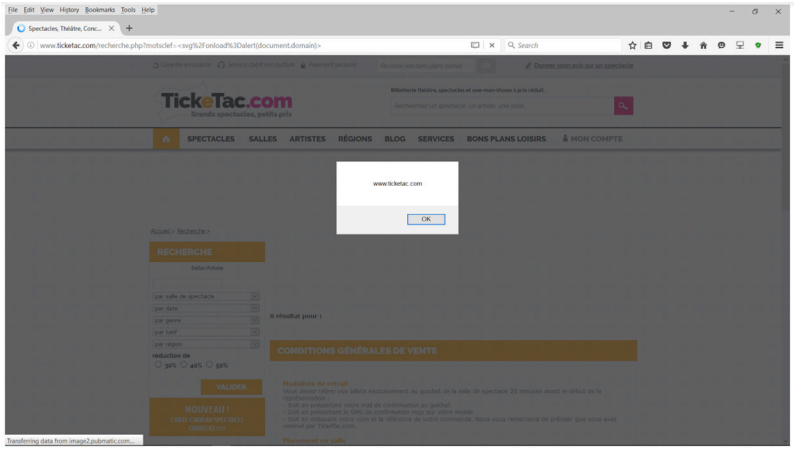
Global impact:
Everyone using the application

Installations:
500,000 - 1,000,000

Android App:
https://play.google.com/store/apps/details?id=fr.lefigaro.ticketac

iOS App:
https://itunes.apple.com/fr/app/ticketac-le-theatre-et-les/id441456353?mt=8

Action required:
Implement encryption



RISK DETAILS

Wandera researchers have discovered data leaks occurring via the registration process that is shared between both SAS Android and iOS apps.

The PII (Personally Identifiable Information) exposed during an account registration include:

- E-mail
- Full Name
- Password

The PII (Personally Identifiable Information) exposed during the login process include:

- E-mail
- Password

The PII (Personally Identifiable Information) exposed during a payment request include:

- Credit Card Type
- Credit Card Number
- Expiration Date
- CVV Number

REMEDIATION AND PREVENTION

Ticketac customers are advised to avoid using the apps over public and potentially insecure Wi-Fi hotspots in order to minimize the risk of traffic interception.

Businesses should have an active mobile security service deployed to block data leaks among any applications that its staff use. A content filtering service is also recommended to limit access to groups of apps and websites, such as gambling.

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

ABOUT WANDERA

Wandera keeps its customers protected from threats like these, either through intelligent blocking of suspicious urls in real-time, or by empowering admins to filter and restrict access to apps or domains that have been compromised.

Our technology examines billions of data inputs every day. With our multi-level architecture, enterprises gain unrivaled visibility into security threats. Because we see more, we prevent more. Enterprises choose Wandera because they know you can only prevent what you can see.

Visit wandera.com/demo to see how your organization could stay protected from these kinds of threats.