wandera

THREAT ADVISORY

Tiscali app

SEVERITY	TYPE	IMPACT	TARGET	REPONSE
3/5	PII LEAK	HIGH	APP	IMMEDIATE

SUMMARY

Wandera's threat research team has discovered a vulnerability in a mobile app created by the well-known telecommunications company Tiscali. This vulnerability is a result of a lack of security in data transmission by the application.

The productivity-focused app allows users to login with their Tiscali e-mail address and password to access their e-mails as well as recent news stories. It also allows individuals to customize the platform to their liking and receive real-time notifications.

Tiscali is a name many are familiar with due to its presence in the Italian market providing telecommunications and internet services. It historically provided internet services across the EU, but has since sold off most of its subsidiaries in areas other than Italy.

SECURITY IMPLICATIONS

Both the iOS and Android versions of the application are using HTTP protocol in order to transmit user information. Specifically, during the login process, users' account names, e-mail addresses, usernames and passwords are being transmitted in plaintext over the internet, making them easily accessible to third parties.

Making matters worse, once users are logged in, the app continuously authenticates them meaning their credentials are leaked multiple times over-the-air. This substantially increases the chances of hackers intercepting the information.

The implications of this app leak are even more concerning when taking into consideration that, with the knowledge of the victim's username and password, a cybercriminal can gain full access to the user's e-mail account. This means any number of malicious attacks can be carried out, including phishing attacks.

RISK DETAILS

Wandera researchers have discovered a data leak occurring during the login process in both the Android and iOS versions of the application.

PII that is exposed when logging into a Tiscali account:

- Account name
- Username
- E-mail
- Password

ABOUT THE TISCALI APP THREAT

What:
A productivity app, created by Italian telecommunications company Tiscali, leaking usernames, passwords and e-mail addresses.

Global impact:
Everyone using the application.

Installations:
100,000 - 500,000 on Android devices, unknown number of iOS downloads.

Android App:
https://play.google.com/store/apps/details?id=com.tiscali.appmail&hl=en

iOS App:
https://itunes.apple.com/us/app/tiscali-it/id1088264929?mt=8

REMEDIATION AND PREVENTION

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

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