wandera

THREAT ADVISORY

iCare Leak

SEVERITY	TYPE	IMPACT	TARGET	REPONSE
3/5	PII LEAK, INSECURE DATA STORAGE, USERNAME ENUMERATION	HIGH	APPS	IMMEDIATE

SUMMARY

Researchers at Wandera have discovered a number of vulnerabilities in a mobile application called “iCare Health Monitor” that put personally identifiable information (PII) and users’ sensitive health metrics at risk. These vulnerabilities are a result of a lack of security in data transit and storage by the application.

iCare Health Studio is a mobile internet company specializing in mobile health service, and provides a mobile application called “iCare Health Monitor”. iCare Health Monitor can measure numerous physiological parameters such as blood pressure, respiratory rate, heart rate, oxygen, vision, hearing, lung capacity and color blindness using only your smartphone.

SECURITY IMPLICATIONS

Both the iOS and Android versions of the application are using HTTP protocol in order to transmit personal user information. Therefore, user credentials, including e-mail, password, sex, age, as well as personal health metrics such as heart rate, are easily accessible to third parties.

Moreover, apart from the lack of data security in transit, it seems the same amount of information is stored on the user’s device in plaintext. Insecure data storage vulnerabilities occur when development teams assume that users or malware will not have access to a mobile device’s file system and proceed with saving sensitive information without any kind of protection. Unfortunately, these systems are easily accessible. When information is not protected properly, specialized tools are all that is needed to view application data.

Lastly, there is a complete lack of a secure session management mechanism which drastically increases the risk of user data leaking. Because of this, an attacker may be able to view the personal data of all registered users only by knowing their email address.

The implications of these potential data leaks leaks could be extremely detrimental on both a personal and enterprise level due the private nature of the information generated by and entered into the application. A malicious third party getting their hands on this data could lead to identity theft, account fraud, and/or implications to personal or enterprise health insurance.

ABOUT THE ICARE THREAT

What:
“iCare Health Monitor”, a mobile application used to measure a number of physiological parameters such as blood pressure, respiratory rate, heart rate, oxygen, vision, hearing, lung capacity, color blindness etc. without requiring any extra devices.

Global impact:
Everyone using the application.

Installations:
500,000 - 1,000,000

Android App:
https://play.google.com/store/apps/details?id=comm.cchong.BloodAssistant

iOS App:
https://itunes.apple.com/us/app/ti-jian-bao-ce-xue-ya-shi/id1062204827

Action required:
Disable HTTP protocol and adopt only HTTPs.

RISK DETAILS

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

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

- E-mail
- Password
- Android OS Version
- Android Device Model
- Sex
- Age
- Metric Type (e.g. Heart Rate)
- Metric Value
- Metric Time

REMEDIATION AND PREVENTION

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

iCare users should have an active mobile security service deployed to monitor for and block data leaks. They are also advised to enable "Device Encryption" on the Android platform so as to protect data at rest.

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 the browser (essentially a workaround). These technologies should have filtering and blocking functionality that happens at the data level to block traffic to leaky apps.

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.