A smartphone app built by China to monitor the health of attendees at the Beijing Winter Olympics next month contains security flaws that makes it vulnerable to privacy breaches and hackers, according to a report released by Canadian researchers on Tuesday.

The MY2022 app was built by the Beijing Organising Committee mainly to track and share COVID-19-related medical information among the athletes during the Games.

Researchers with Toronto’s Citizen Lab project said MY2022 failed to properly encrypt the transfer of personal data, leaving it vulnerable to hackers. They also found that MY2022’s privacy policy does not specify which organisations it would share the users’ information with.

The International Olympic Committee (IOC) said it had conducted independent assessments on the application and had not found any “critical vulnerabilities”.

“It is not compulsory to install ‘My 2022’ on cell phones,” the IOC said in a statement.

Yu Hong, the director general of the committee’s technology department, said on Wednesday that the main function of the app is to monitor people’s health and the country follows strict rules to protect data.

All of the MY2022 app’s technology aspects have been validated by relevant app stores, the Beijing 2022 official said at a briefing hosted by the Chinese embassy in the United States. She was speaking via video from Beijing.

Yu also said that technology vulnerabilities were natural when developing this kind of an app, which her department was constantly updating in order to remove such issues.

The Citizen Lab researchers said they found the flaws in the iOS version of the app after creating an account in it. They were unable to set up an account in the Android version but said the security flaws existed in both versions of MY2022.

The report said MY2022 failed to validate SSL certificates, which are needed to authenticate a website’s identity and enable encrypted connection. This can be exploited by hackers to transmit the data to malicious sites.

Non-encrypted data is transmitted to “tmail.beijing2022.cn” by MY2022.

“Such data can be read by any passive eavesdropper, such as someone in range of an unsecured WiFi access point, someone operating a WiFi hotspot, or an Internet Service

Provider or other telecommunications company,” the report said.

Citizen Lab said it had informed the Beijing Winter Olympics Organising Committee on Dec. 3 of its security concerns but had not received any response.

The Winter Olympics are set to begin on Feb. 4. Several countries including the United States, Britain, Japan and Australia have announced diplomatic boycotts of the Games over concerns about human rights in China.

*Reporting by Ann Maria Shibu in Bengaluru, Martin Pollard in Shanghai and Beijing Newsroom; editing by Ed Osmond and Michael Perry*

*The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team*

Facebook Comments