Chair of Connected Mobility
TUM Department of Informatics
Technical University of Munich

Vulnerabilities in the MY2022 Olympia App

Fabian Höltke, Sven Andabaka, and Maximilian Geitner

TUM Department of Informatics, Technical University of Munich

February 07, 2022

1 Introduction

The MY2022 application is required for all attendees of the Beijing 2022 Olympics and has common features such as news and weather updates for the event, but also features for device tracking, health monitoring, health custom clearance, audio chat, or file transfers. These features contain highly sensitive user data, therefore the Citizen Lab from the University of Toronto has analyzed the application's data collection and its privacy behavior [1].

2 Privacy Infringement

Some of the MY2022 app features use sensitive user data. One example is the health custom clearance process which involves passport details, demographic information, travel, and medical information. For the event, the user needs to do self-reports on the health status, register the COVID-19 vaccination status as well as COVID-19 lab test results.

Besides the data collection from the Beijing Organizing Committee and government-related organizations, there is also data traffic to third-party services from Tencent, Weibo, and iFlytek for information sharing, location services, or translation services. These services can be problematic for the user's privacy because they involve device unique identifiers, real-time location, audio information, device storage access, and other device-related data. Notably, the iFlytek module for AI audio translation services is banned in the US due to the mass surveillance capabilities on ethnic minorities in China [5].

Jonathan Scott, a US security researcher, decompiled the MY2022 app and analyzed the application regarding data traffic and permissions[2]. In the Android application, there are permission requests for contacts, the camera, the microphone, and many others. Also, the application might be able to process commands from remote to start simple tasks like retrieving the clipboard data, system information, or changing network settings.

3 Vulnerabilities in Data Transmission

There are two major vulnerabilities regarding data transmission. The first one is that some part of sensitive data is not encrypted at all while transmitting. The second one is that the SSL certificate pinning was incorrectly implemented leading to a failure of validating SSL certificates at all. Both these vulnerabilities lead to the problem that third parties can sniff the network traffic through a man-in-the-middle attack and see sensitive transmitted data.

3.1 Failure to encrypt sensitive data

The Canadian researchers found out that the app sends non-encrypted data to the mail-related API endpoint. Doing so, it sends sensitive metadata regarding the chat functionality, including the user ID of the sender and receiver. Therefore, an attacker would be able to trace with whom the victim was in contact.

3.2 Failure to validate SSL certificates

A common bug when developing applications is to forget about or implement incorrect SSL certificate validation. SSL certificates themselves just encrypt the data traffic, but cannot assure that the client is communicating with the correct server. Without validating SSL certificates man-in-the-middle attacks can not be prevented.

Again, the Canadian researchers found out that some of the API endpoints are malicious. They were able to find five servers, where no correct certificate pinning was implemented. Especially one endpoint (health.customsapp.com), used for transmitting health data and travel information, was not secured properly. This leads to the fact that an attacker could sniff sensitive information of the athletes and misuse their data.

4 Censorship Analysis

Like many other Chinese published apps, MY2022 ships with a user reporting feature and a so-called „illegal words"-list. The list contains 2,442 keywords,

which are mainly politically motivated or social content referencing pornography. The words originate mainly from simplified Chinese, with a small portion in Tibetan, Uyghur, traditional Chinese, and English. However, the referenced research could not detect where the list is exactly applied. All performed tests indicate that the censorship list is not used in the current versions. Only the user reporting feature, which can flag content as politically sensitive, seems to be used as the only censoring tool in the app.

5 Conclusion

It is unclear why the censorship list was not applied in the app. The authors suspect that pressure from foreign governments or the IOC may be the reason for this. The IOC previously debated with China about the extent to which censorship could be applied at the Olympics [4].

Also, it is not clear if the data-transmission vulnerabilities are included on purpose or if they are just human errors. It is quite possible that the developers left these vulnerabilities on purpose as it is common practice in China to use data interception technology. Businesses, such as cafes and universities, are responsible for their network traffic and therefore tend to sniff WiFi traffic. These vulnerabilities violate regulations from Apple's security guidelines, the terms of the Google Play Store, and even Chinese Privacy Laws [1].

Additionally, suspicions about privacy infringements of the MY2022 app could not be resolved, even after having a closer look at the decompiled app. It can be seen that the app allows external attackers to trigger functions for data collection and device state changes.

As a consequence, several nations, including the US and Germany, gave athletes burner phones. They suggested that athletes should not bring their personal phones to the games [3] [6].

References

[1] Cross-Country Exposure analysis of the MY2022 olympics app. https://citizenlab.ca/2022/01/cross-country-exposure-analysis-my2022-olympics-app/. Accessed: 2022-02-07.

[2] Decompiled 2022 beijing olympics apps. https://github.com/jonathandata1/2022_beijing. Accessed: 2022-02-07.

[3] Olympische Spiele in China: Athleten sollen eigene Handys nicht nutzen. https://www.heise.de/news/Olympische-Spiele-in-China-Athleten-sollen-eigene-Handys-nicht-nutzen-6328104.html. Accessed: 2022-02-07.

[4] Update 1-olympics-ioc admits to deal with china on censorship. https://web.archive.org/web/20210507010002/https://www.reuters.com/article/olympicsNews/idUSPEK15086520080730. Accessed: 2022-02-07.

[5] U.S. expands blacklist to include china's top AI startups ahead of trade talks. https://www.reuters.com/article/us-usa-trade-china-exclusive/u-s-expands-blacklist-to-include-chinas-top-ai-startups-ahead-of-trade-talks-idUSKBN1WM25M. Accessed: 2022-02-07.

[6] Why fbi doesn't want US athletes using their phones during beijing olympics 2022. https://www.theinfographicsshow.com/why-fbi-doesnt-want-us-athletes-using-their-phones-during-beijing-olympics-2022/. Accessed: 2022-02-07.