Summary

The Citizen Lab is an academic research group based at the Munk School of Global Affairs & Public Policy at the University of Toronto in Toronto, Canada.

We analyzed Samsung Keyboard on Android as part of our ongoing work analyzing popular mobile and desktop apps for security and privacy issues. We found that Samsung Keyboard for Android includes a vulnerability that allows network eavesdroppers to recover the plaintext of insufficiently encrypted network transmissions, revealing sensitive information including what users have typed.

Device	**File name**	**Version analyzed**
Samsung SM-T220 T220ZCS4CWF4 / T220CHN4CWF4	HoneyBoard.apk	5.6.10.26

Table 1: The version of Samsung Keyboard analyzed.

Findings

We found that when using Samsung Keyboard on the Chinese edition of a Samsung device (in our testing, an SM-T220 running ROM version T220CHN4CWF4) and when Pinyin is chosen as Samsung Keyboard's input language, Samsung Keyboard transmits keystroke data to the following URL via HTTP POST:

```
http://shouji.sogou.com/web_ime/mobile_pb.php?durtot=339&h=8f2bc112-bbec-3f96-86ca-652e98316ad8&r=android_oem_samsung_open&v=8.13.10038.413173&s=&e=&i=&fc=0&base=dW5rbm93biswLjArMC4w&ext_ver=0
```

The keystroke data is contained in the request's HTTP payload in a protobuf serialization (see Figure 1 below).

```
1 {
  1: "8f2bc112-bbec-3f96-86ca-652e98316ad8"
  2: "android_oem_samsung_open"
  3: "8.13.10038.413173"
  4: "999"
  5: 1
  7: 2
}
2 {
  1: "\351\000"
  2: "\372\213"
}
4: "com.tencent.mobileqq"
7: "nihaocanyoureadthis"
16: 10
17 {
  3 {
    1: 1
    2: 5
  }
  5: 1
  9: 1
}
18: ""
19 {
  1: "0"
  4: "339"
}
```

Figure 1: Protobuf transmitted after typing “nihaocanyoureadthis”.

The device on which we were testing was fully updated on the date of testing (October 7, 2023) in that it had all OS updates applied and had all updates from the Samsung Galaxy Store applied.

Vulnerability

Samsung Keyboard transmits keystroke data via plain, unencrypted HTTP, and there is no encryption applied at any other layer either. Therefore, a network eavesdropper who is monitoring a Samsung Keyboard user’s network traffic can easily observe that user’s keystrokes if that user is using the Chinese edition of the ROM with the Pinyin input language selected.

Mitigation

In order to address the reported issue, Samsung Keyboard should secure all transmissions using a popular, up-to-date implementation of HTTPS or, more generally, TLS instead of transmitting sensitive user data in the clear.

We previously disclosed a similar vulnerability to Tencent concerning the app Sogou Input Method, which also transmitted keystroke data insecurely to `*.sogou.com` servers. In the disclosure, we recommended that Tencent secure their transmissions using TLS, and Tencent subsequently adopted changes to transmit keystroke data in future versions of the app using HTTPS.