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 Vivo's pre-installed keyboard apps as part of our ongoing work analyzing popular mobile and desktop apps for security and privacy issues. We found that the Sogou-based one includes vulnerabilities that allow network eavesdroppers to decrypt network transmissions from the keyboards. This means that third-parties can obtain sensitive personal information, including what users have typed.

Platform	**Keyboard name**	**Package Name**	**Version analyzed**
origin OS 3	搜狗输入法定制版	com.sohu.inputmethod.sogou.vivo	10.32.13023.2305191843

Table 1: The versions of the Vivo keyboard apps analyzed which were vulnerable.

Findings

The Sogou-based keyboard app is vulnerable to a vulnerability which we have already publicly disclosed in Sogou Input Method (搜狗输入法) in which a network eavesdropper can decrypt and recover users' transmitted keystrokes. Please see the corresponding details in this report for full details. Tencent responded by securing Sogou Input Method transmissions using TLS, but we found that 搜狗输入法定制版 (com.sohu.inputmethod.sogou.jovi) remains unfixed.

Mitigation

In order to address the reported issues, Vivo should secure keyboard app transmissions using a popular, up-to-date implementation of HTTPS or, more generally, TLS instead of relying on custom-designed cryptography to secure the transmission of sensitive user data.

We previously disclosed a similar vulnerability to Tencent (腾讯) in their corresponding keyboard app Sogou IME (搜狗输入法). Tencent responded by securing Sogou Input Method transmissions using TLS.