UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Alibaba (China) Co., Ltd
969 West Wen Yi Road
Yu Hang District
Hangzhou 311121
China

June 3, 2016

Dear Madam or Sir,

Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, is currently researching the security and privacy features of UC Browser (Windows and Android versions). As you know, on April 13, 2016 we notified Alibaba of the security vulnerabilities we discovered in the browser, and we have been in communication with Alibaba engineers since that date. We write now concerning the status of the fixes, as well as broader issues of user privacy and access to information implicated in the browser's design.

We would appreciate your timely response to the following questions:

1. UC Browser (Android versions 10.9.0.7013, 10.2.1.161 and 7.9.3.103; Windows version 5.5.10106.5) collects detailed and extensive user data, as documented in our correspondence. Why is this sensitive user data collected? Why is it transmitted insecurely?
2. Which laws, regulations or policies (internal or external) govern Alibaba/UCWeb's collection of user data? What user data is Alibaba/UCWeb required to collect pursuant to such law, regulation or policy?
3. Does Alibaba/UCWeb intend to alter its collection through UC Browser of certain types and amounts of user data? If so, what changes will be made, and when?
4. For how long does Alibaba/UCWeb retain the user data that it collects through UC Browser? How is the data stored, and what security measures are in place to protect that data at rest? Does Alibaba/UCWeb share that data with third parties? If so, with whom?
5. What if any laws, regulations or policies (internal or external) guide Alibaba/UCWeb in the use of encryption in transmitting or storing user data?

6. Why was UC Browser designed to use symmetric encryption and hard-coded keys, rather than asymmetric encryption?
7. When will the Android version of UC Browser transition to HTTPS to encrypt traffic sent to the search suggestion and update servers?
8. Has Alibaba/UCWeb investigated if any other personal user data is transmitted via insecure means beyond those for which we have notified you?
9. Why does version 10.10.0.800 of UC Browser for Android obfuscate an insecure encryption implementation (libsgmain.so)?
10. Since other Androids apps developed by Alibaba (including Ali Pay, Ali Shopping and Taobao) contain libsgmain.so, do they also transmit sensitive data insecurely? If so, can you provide a timeline for when these apps will be fixed?
11. What steps will you take to ensure that no data leaks remain in UC Browser? What steps will you take to ensure that no data leaks will be introduced into UC Browser in the future?

We plan to publish a report reflecting our research no sooner than June 10, 2016. We would appreciate a response to this letter from your company as soon as possible, which we commit to publish in full alongside our research report. Thank you.

Sincerely,

Professor Ronald J. Deibert
Director of the Citizen Lab
Munk School of Global Affairs
University of Toronto