PERINGATAN: APLIKASI ZOOM BERHADAPAN DENGAN ISU KESELAMATAN DAN PENDEDAHAN DATA PENGGUNA

Aplikasi ini dilaporkan menghantar data pengguna iOS ke Facebook walaupun pengguna tidak mempunyai akaun Facebook. Ia didakwa menyediakan data kepada Facebook apabila pengguna membuka aplikasinya dimana ia termasuk model peranti yang digunakan, zon masa dan bandar pengguna, serta lain-lain yang boleh digunakan untuk mensasarkan iklan.

Zoom menyatakan mereka hanya mengumpul data pengguna yang perlu untuk meningkatkan perkhidmatan termasuk alamat IP, butiran OS, dan butiran peranti. Akan tetapi, ia tidak membenarkan pekerjanya mengakses kandungan tertentu mesyuarat serta tidak menjual apa-apa jenis data pengguna.

Selain itu, pengguna Zoom turut terdedah kepada ciri yang ada pada aplikasi tersebut dimana ia membolehkan penyerang mencuri data pengguna. Perkara itu didedahkan oleh seorang penyelidik keselamatan yang mendapati klien Zoom akan menukarkan rangkaian Windows UNC *path* kepada pautan yang boleh diklik dalam mesej.

Ini bermakna, apabila pengguna menekan pautan tersebut, secara *default* Windows akan menghantar nama dan kata laluan log masuk pengguna, di mana ia boleh digodam dengan mudah menggunakan *tool* percuma seperti Hashcat untuk mendedahkan kata laluan pengguna.

Dalam pada itu, Zoom turut berhadapan dengan isu *end-to-end encryption.* Ini kerana, jika dilihat pada laman web atau Zoom Security White Paper, Zoom menyatakan

bahawa syarikat itu menyokong *end-to-end encryption*. Namun, melalui penyelidikan oleh The Intercept mendedahkan perkara tersebut adalah tidak benar.

Artikel ini di keluarkan bagi tujuan peringatan dan langkah berjaga-jaga.

Sumber: MyTech Decisions, BleepingComputer, The Verge

Dikeluarkan oleh:
Jabatan Pengurusan Maklumat
7 April 2020