PHYS.ORG

Many fitness trackers leak personal data: study

July 18 2016

Xiaomi fitness tracker

Security weaknesses on many popular fitness trackers may allow hackers to access or potentially manipulate user data, a study showed Monday.

The study of seven Android-powered trackers by the security firm AV-Test showed vulnerabilities similar to that found in its research from a year earlier—with many devices lacking secure connections or tamper protection.

The researchers said the Apple Watch, which was evaluated using different criteria because of its operating system, had a "high security rating" despite some "theoretical vulnerabilities."

The seven Android devices showed varying levels of security, with some allowing hackers the ability to access or tamper with user data.

"As already witnessed in the initial test of fitness wristbands last year, many manufacturers are also committing similar errors in the current test," the report said. "They often don't pay sufficient attention to the aspect of security."

The highest risk came from devices made by Runtastic, Striiv and Xiaomi, with seven to eight potential vulnerabilities out of 10.

"These products can be tracked rather easily, use inconsistent or no authentication or tamper protection, the code of the apps is not sufficiently obfuscated (to secure data), and data traffic can be manipulated and monitored with root certificates," the report said.

"Worst of all, Xiaomi even stores its entire data unencrypted on the smartphone."

The researchers noted that security should be taken more seriously as fitness trackers move beyond the casual athlete, and health insurers use such devices to set rates or offer discounts.

According to research firm IDC, the number of fitness trackers sold worldwide topped 75 million in 2015 and in 2016 the number is expected to exceed 100 million.

The most secure devices in the test, with two to three potential security risks, were the Pebble Time, Microsoft Band 2 and Basis Peak.

The Apple Watch, the report said, is "almost impossible to track," but in airplane mode it reveals certain identifying characteristics which "should actually not be the case."

The Apple device "mostly uses encrypted connections that are additionally secured," but its updates are made through an unencrypted connection, the researchers said.

Citation: Many fitness trackers leak personal data: study (2016, July 18) retrieved 24 April 2024 from https://phys.org/news/2016-07-trackers-leak-personal.html