Issued 10/20/17

Security Flaws in Children's Smartwatches Make Them Vulnerable to Hackers

Internet connected smartwatches for children have been found to contain security vulnerabilities which allow hackers access to track the wearer's location, eavesdrop on conversations or even communicate with the child user. And with some of these devices, data is transmitted and stored without encryption.

The investigation came to the conclusion that the Xplora smartwatch, the Viksfjord smartwatch and the Gator 2 smartwatch - and their associated apps contained unacceptable security vulnerabilities. Findings differed between watches, but tests showed how unauthorized people could access functions in the apps and watches through "various forms" of attack.

Flaws included allowing information about the child's location to be revealed, provided unauthorized access to accounts and allowing attackers to manipulate the information given to the parents about the child's location.

In addition to the security flaws, a common theme across all watches tested is that none of the companies behind them asked for consent to the processing of personal data when setting up an account, with Gator 2 failing to supply terms of use.