BEUC The European Consumer Organisation

Press Release

Contact: **Sébastien Pant: press@beuc.eu | Mob: +32 (0)470 13 47 38**
Date: **19/07/2023**
Reference: **BEUC-PR-2023-033**

Cybersecurity of connected consumer products insufficiently addressed by EU Parliament

The European Parliament's Industry Committee (ITRE) in the lead for the Cyber Resilience Act, a proposal to set minimum cybersecurity requirements for connected products, has, through today's vote, tightened some obligations for manufacturers, but ultimately failed to tackle all its major blind spots.

Consumer groups from the BEUC network have repeatedly raised the alarm about the poor cybersecurity of connected products.[1]

It is positive that the ITRE Committee has required sensitive consumer products, such as smart home systems or connected toys, to go through a more rigorous assessment that they conform to the law. However, the committee fell short of requiring this assessment to be carried out by an independent third-party, which BEUC called for. Going through an independent third-party assessment would ensure more demanding product testing and thus increase the likelihood that security vulnerabilities are detected before the item is placed on the market.

Regrettably, the committee also ignored our calls for manufacturers to have to continuously address security vulnerabilities by providing software updates for the product's expected lifespan.

It is at least positive the ITRE Committee has given consumers a right to go to court as a group to seek compensation if the product they all bought did not meet cybersecurity standards.

Ursula Pachl, Deputy Director General of the European Consumer Organisation, said:
"Connected products are in our homes and in our pockets, yet the market has failed to adequately protect us against cybersecurity risks. This is why we need regulation to make sure consumer products like smart door alarms and children's dolls comply with minimum cybersecurity requirements for manufacturers.

"While the Parliament has made some improvements, for example by requiring that sensitive consumer devices go through more rigorous conformity assessments for cybersecurity, they should have done more. For example, it is crucial that all connected products receive software updates for their entire lifespan. Consumers expect that the products they buy are not only safe but stay secure throughout their lifetime, which for products such as a dishwasher can be thirteen years or more.[2] Otherwise, connected products can become a liability at a certain point even though they still function. This would be bad for consumers' pockets but also encourage electronic waste, which is at odds with the EU's sustainability goals."

ENDS

[1] In 2016, the #ToyFail campaign, launched by our Norwegian member Forbrukerrådet, showed that a children's doll named Cayla could be easily hacked in just a few simple steps. Test Achats/Test Aankoop from Belgium installed 19 popular smart home devices (including a smart fridge, alarm system and a door lock) and challenged two ethical hackers to find security vulnerabilities. They found problems with more than half the products.

[2] Which? 'Smart' TVs and washing machines may be abandoned by brands after two years' (January 2023)

Co-funded by the European Union