Press Release

Contact: **Sébastien Pant: press@beuc.eu**
Date: **15/09/2022**
Reference: **BEUC-PR-2022-039**

Cybersecurity of connected products could improve significantly following Commission proposal

The European Commission has proposed new rules for the cybersecurity of connected products which would substantially improve the worrying situation today. This proposal answers a longstanding need that the BEUC network identified and warned about repeatedly.

Too many consumer-facing products lack even basic cybersecurity features, leaving consumers exposed to cyberattacks. The rules proposed today would establish mandatory security requirements for products as diverse as connected toys, PCs or smartphones. Manufacturers would be obliged to ensure that products are cybersecure by design and by default, provide encryption, software and security updates and strong authentication mechanisms.

However, the proposal needs to be improved to meet consumer needs, for example by recognising the need for independent third-party assessment of certain products that pose higher risks to consumers, such as smart home systems, which can endanger the homeowner if hacked. The proposal should also require manufacturers to continuously address security vulnerabilities by providing software updates for the product's expected lifespan. There should also be more effective redress and compensation mechanisms for consumers who are harmed by a product not meeting cybersecurity requirements.

Ursula Pachl, Deputy Director General of the European Consumer Organisation, said:
"We are using more and more connected products in our lives, yet many of them do not even have the most basic cybersecurity features. The market has failed to deliver on cybersecurity, placing consumers at risk. Whether it is a connected toy which gets hacked and allows a stranger to speak to our child, or a smart home alarm that gets disabled, consumers need to be able to rely on the fact that connected products they buy are safe and secure.

"Today's proposals mark a welcome break in the reality of poor cybersecurity for consumer products, but we need further improvements to make this law deliver fully for people. For example, certain consumer products, such as children's devices, smart home systems, security devices or internet routers should be classified as high risk and require certification from third parties. Manufacturers should also tackle cybersecurity vulnerabilities during a product's expected lifespan. Consumers also need to have more effective redress mechanisms at their disposal to get fair compensation when things go wrong."

Background
Consumer groups part of the BEUC network have repeatedly raised the alarm about poor cybersecurity in connected products. Already in 2016, the #ToyFail campaign, launched by our Norwegian member Forbrukerrådet, showed that a children's doll named Cayla could

This press release is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).

be easily hacked in just a few simple steps [1]. Test Achats/Test Aankoop from Belgium installed 19 popular smart home devices (a smart fridge, alarm system, door lock, etc.) and challenged two ethical hackers to find security vulnerabilities. They found problems with more than half the products. [2]

ENDS

[1] Forbrukerradet, 'Connected toys violate European consumer law' (December 2016, accessed 15 Sept 2022)
[2] Test Achats/ Test Aankoop, 'Attention aux voleurs numériques' (August 2021, accessed 15 Sept 2022)

If you would like to be removed from our mailing list, please let us know.

Bureau Européen des Unions de Consommateurs AISBL | Der Europäische Verbraucherverband
Rue d'Arlon 80, B-1040 Brussels ○ Tel. +32 (0)2 789 24 01 ○ press@beuc.eu ○ www.beuc.eu ○ www.twitter.com/beuc
TVA: BE 0422 071 051 ○ EC register for interest representatives: identification number 9505781573-45

This press release is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).