KEYSIGHT

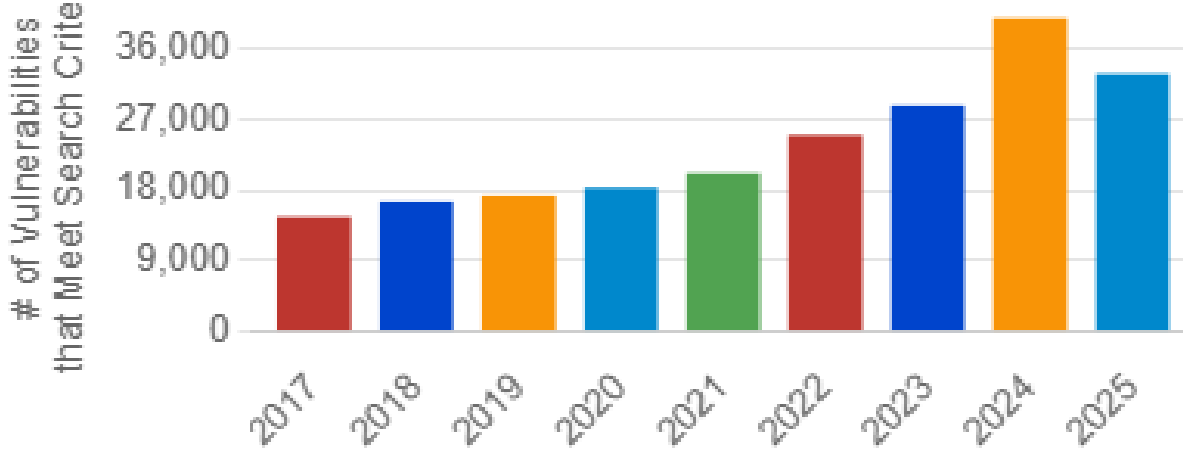
Cyber Resilience Act (CRA) Impact on Open Source

CHES Optimist 13 September 2025
Marc.Witteman@keysight.com

CRA impact on digital products

- Estimated **€10 billion in annual costs** from product vulnerabilities in the EU
- The EU addresses this problem in the Cyber Resilience Act, which will be enforced as of 2027
- The CRA act requires that products are and remain free of exploitable vulnerabilities
- Product vendors that want to bring products to the EU market will have to be compliant (or accept the risk of fines)
- Pure open-source products are excluded,
  but commercial products containing open-source (>90%) are not

CRA impact on Open-Source



- Growing number of known (and unpatched) vulnerabilities are collected in CVE databases
- Unpatched vulnerabilities in open-source must be addressed by product vendors,
  Two choices available (if the vendor wants to be compliant):
  1. Make a contribution to open-source
  2. Make a proprietary solution

An existential challenge for Open-Source

Open-Source contribution

- Pro
  - Community benefit
- Con
  - Complexity

Proprietary solution (fork or redevelopment)

- Pro
  - Competitive differentiation
- Con
  - Open-source becomes bugware

How can we encourage product vendors to contribute to open-source?

KEYSIGHT

Thank you