The Cyber Resilience Act: How to make Europe more digitally resilient?

With contributions from EDRi members

epicenter.works, Austria
Electronic Frontier Foundation , US
Free Software Foundation Europe, EU
Privacy International, Global
Vrijschrift.org, Netherlands

EXECUTIVE SUMMARY

We welcome the aim of the Cyber Resilience Act (CRA) to bolster cybersecurity rules and to ensure more secure hardware and software products. Nevertheless, we note that the proposal put forward by the European Commission contains a number of serious shortcomings which would both hamper digital innovation and harm people who increasingly rely on digital products and services.

It is essential that these shortcomings are effectively addressed by EU co-legislators to ensure that the aim of the Regulation is not undermined, and that people's devices and data remain secure in our connected world.

In order to address these problems, the Cyber Resilience Act should:

1. **Require 10 years worth of software security updates from device manufacturers;**
2. **Exempt free and open source software projects that are provided not-for-profit or by micro-enterprises from the burden of the Regulation;**
3. **Increase the transparency of security vulnerability handling and disclosure;**
4. **Include a criminal and civil liability safe harbour for vulnerability handling and disclosure practices of good faith security researchers.**

The proposed Regulation should be improved to ensure that current practices do not result in serious harms to people or negatively impact our devices' sustainability and digital innovation in the open source space that underpins the large majority of today's software stack.

1. MANDATE LONG-TERM SOFTWARE SECURITY UPDATES

Up-to-date software is what enables our devices to function, keeps them compatible with the latest apps, and secures them against known vulnerabilities. Outdated and unmaintained software on an otherwise functioning device can enable malicious actors to break into your bank account or the intimacy of your private life; and worse: it can endanger your life and physical safety. Such risks are enabled by software support periods that are much shorter than the product's possible life cycle. They are the result of an industry more interested in selling new devices than in providing long-term software support for their existing products.

Under its Circular Economy Action Plan 2020 and the European Green Deal, the EU wants mobile phones and other devices to be durable, easily repairable by consumers, and reusable for as long as possible. That's why the latest EcoDesign Proposal puts forward an obligation for manufacturers to allow consumers to more easily replace smartphone and tablet batteries.

Yet, a longer hardware life will fail to have any impact if device manufacturers stop providing software security fixes after a short period of time. That is particular problematic for devices that consumers could and want to use for a long period of time, such as smartphones, tablets, and 'smart' home appliances like TVs, fridges and washing machines.[1]

What is more, at the time of purchase, there is currently no transparency of how long a given new device will receive software security updates. Research shows how the current software support landscape is characterised by varying and inconsistent approaches to security updates, with support periods being undisclosed or differing by product category and over time. Even where this information is disclosed to consumers, it is often hard to find without combing through legal texts or online forums. This practice leads to manufacturers selling devices in large numbers with out-of-date software at the expense of Europe's digital security and cyber resilience.

SOLUTION: Given the increasing lifetime of hardware as well as the ecological need to reduce e-waste, the minimum time period during which device manufacturers must provide software security updates (Article 10(6) CRA) should be set to 10 years. Any shorter duration of security software support would hamper innovation, reduce competition, and result in premature obsolescence and increased e-waste.[2] To increase transparency, a mandatory and clearly visible product label on each consumer-facing packaging should indicate the device's end-of-support date.

1 A YouGov survey commissioned by PI in 2022 shows that consumers expect their smartphones, computers, smart TVs and gaming consoles to receive security updates for a much longer period than what several manufacturers actually provide, leaving consumers with expensive tech that is vulnerable to malfunctions and hacking attacks.

2 Europe is the world's largest e-waste producer per capita (16.2 kg). The EU's recycling schemes do not keep up with the rate of new e-waste generated by too short life cycles of devices and few repair options.

2. EXEMPT ESSENTIAL OPEN SOURCE SOFTWARE FROM THE SCOPE

The CRA as proposed is intended to exempt open source software projects that are provided not-for-profit or by micro-enterprises from the regulatory requirements. Such an exemption is important because free and open-source software (FOSS), like Firefox, Signal and Linux, play an essential role in Europe's software ecosystem.

But the exemption proposed by the Commission is too narrowly limited to open source software that is entirely non-commercial. As soon as a FOSS project accepts donations or receives a small revenue to support or sustain its development, for example by providing support services to users, they would fall out of the exemption no matter how tiny the amounts involved.

That overly expansive wording of 'commercial activity' in Recital 10 of the proposal would strip away the limited but sustainable methods of financing the development work that makes FOSS more secure and stable, while maintaining their open source nature that underpins trust and confidence in those essential pieces of software. Similar views have been voiced by over a dozen expert stakeholders including The Document Foundation, the Open Source Initiative and also industry players like Microsoft, DigitalEurope and Bitkom.

Throwing small open source software projects out of the exemption would also disincentivise their professionalisation. Too often, small but crucial projects like the password manager Keepass (used by EU institutions) or OpenSSL (which enables secure connections to online banking) are maintained by highly skilled volunteer developers, sometimes with small business operations attached to it. Making their development sustainable and enabling steady streams of (limited) revenue is a key stepping stone for digital security and sovereign innovation in this area.

Faced with increasing compliance burden, FOSS maintainers may switch to a proprietary closed-source model (to guarantee the income required for compliance) or abandon essential software projects entirely (to avoid compliance risk). Either would be a huge loss for the innovative strength of the EU's software market. It would put many downstream products that rely on FOSS in peril and reduce software security by shutting down transparent development best practices.

SOLUTION: The CRA should replace the concept of "commercial activity" with an approach that focuses on deployment and the entity that benefits on the market. Therefore an exemption of non-profit entities and micro-enterprises that publish or deploy free and open source software should be introduced in the substantive part of the Regulation (instead of the recitals). That way, all FOSS solutions with a significant impact on the EU's cyber resilience are covered by the CRA specifications, while the compliance burden is carried by those market players that enjoy the largest profits from their use.

3. INCREASE TRANSPARENCY OF SOFTWARE VULNERABILITY HANDLING

Cyberattacks targeting products with digital elements often leverage known and fixed vulnerabilities in devices that have not been updated (see point 1 above on 10-year software support). In an effort to enforce a common and coherent handling of software vulnerabilities, the CRA proposal imposes obligations on manufacturers to promptly notify the EU Agency for Cybersecurity (ENISA) of any actively exploited vulnerabilities contained in products with digital elements (Article 11), which would in turn inform the respective market surveillance authority.

While we welcome those requirements for proprietary software vendors, they do little to enforce *public transparency* around fixed software vulnerabilities. It also fails to create an EU best practice of coordinated vulnerability handling and disclosure.

In order to increase public accountability and transparency, software manufacturers should be obliged to publicly disclose and describe any vulnerability that has been fixed as part of the product's change log or release notes. This is in line with current digital security best practices that have been applied as part of the internationally recognised Common Vulnerabilities and Exposures (CVE) system, which provides a reference method for publicly known vulnerabilities. This would increase digital security by enabling customers, other market participants, and the public to obtain a history of vulnerabilities and evaluate the long-term quality and trustworthiness of a software product on the EU market.

At the same time, Annex I requires the delivery of software "without any known exploitable vulnerabilities" which risks to be an unobtainable objective. Many software developers regularly learn of new vulnerabilities and make risk-based assessments on the need to prioritise fixes for timely delivery of software updates. In many cases, vulnerabilities may be identified that do not affect the security of a piece of software in practice because, for example, they may only be exploitable in environments where the product is not intended to be used.

Instead, the CRA should require software vendors to fix known vulnerabilities as quickly as possible, typically within a period of 90 days. But it should also be possible to extend this time period in cases of low severity vulnerabilities, which should enable developers to prioritise high-risk vulnerabilities, for instance those allowing remote code execution on widely used devices, over lower-risk vulnerabilities with little practical exploitability.

SOLUTION: Add a clear and mandatory EU standard of coordinated vulnerability handling and disclosure as certification requirement. That standard should include a 90-day default period for eliminating known vulnerabilities, with extensions possible for low-risk cases, as well as obligatory public disclosure after the fact, unless such disclosure would harm the public interest.

4. PROTECT GOOD-FAITH SECURITY RESEARCH PRACTICES

Every IT product can contain security vulnerabilities unknown to the vendor. Often, these vulnerabilities are discovered by security researchers, who must decide how to handle this critical knowledge. Their options include (1) commercial exploitation of the vulnerability, (2) not informing anyone, or (3) informing the vendor about the flaw. The third option – in conjunction with withholding publication within a reasonable time to repair the vulnerability – is often in the public's best interest.

With few exceptions in some EU member states, however, this socially beneficial course of action does not provide benefits to the security researcher. On the contrary, researchers might even face legal repercussions for discovering the vulnerability in the first place. Even when acting in good faith, such as by informing the vendor and avoiding public disclosure until the vulnerability is fixed, researchers are rarely protected against criminal or civil liability lawsuits, a practice at odds with much-needed national or EU-level bug bounty programmes that encourage security research.

The legal risks security researchers face is detrimental to the security of Europe's IT products and systems. History has shown that vulnerabilities are often discovered by outside reviewers, and those actors play a critical role in increasing the security of real-life operational and widely deployed systems. If independent security researchers are not contracted by vendors, the legal risk of disclosing security vulnerabilities becomes a determining factor in the decision how to handle a particular discovery. The risk of liability can have a chilling effect that deters them from any form of disclosure at all, making everyone less safe.

SOLUTION: The EU's ultimate goal should be to provide criminal and civil liability protections and establish a safe harbour for good faith security researchers whose research and disclosure shows no criminal intent. A safe harbour could be designed along the lines of the EU Whistleblower Directive by protecting disclosures to certain contact points (public authority or vendor), while withholding public disclosure for a reasonable time that allows for the repair of the system.

In the CRA a meaningful step towards this goal is to include coordinated disclosure obligations for vendors as part of their certification. Such an obligation would provide security researchers that report vulnerabilities to vendors the assurance that they will be listened to and coordinated with.