EU Cyber Resilence Act moves to next stage, “impending tragedy” for open source?

By **Tim Anderson** - July 21, 2023

Security resilience

The Council of the EU has agreed a common position on the Cyber Resilience Act (CRA), which introduces mandatory cybersecurity requirements for hardware and software, despite the strong concerns of the open source community including the Apache Software Foundation (ASF) which called it an “impending tragedy.”

The meeting of the Council on 19th July agreed a “negotiating mandate” for the CRA, which empowers the Spanish Presidency to negotiate with the European Parliament on the final version of the legislation. This negotiation is called the trilogues, as it involves the European Commission, the European Parliament, and the Council of the EU.

MEP’s on the Committee on Industry, Research and Energy (ITRE) approved a draft CRA by 61 votes to 1, with 10 abstentions.

The purpose of the legislation is to provide common security requirements for connected devices, such as IoT (Internet of Things) products, so that they are “secure thoughout the whole supply chain and throughout their whole life cycle.” It is a worthy goal, aiming to end the blight of devices running insecure firmware that cannot easily be updated, or whose vendors pay little attention to the security of products that are no longer on the market. The legislation includes a CE marking to indicate conformity, hence it is sometimes called a “CE mark for software.”

As we reported earlier this year, open source advocates and maintainers are anxious about unintended consequences and unaffordable costs imposed on projects which provide free software.

> Those concerns have not diminished, with Dirk-Willem van Gulik, VP Public Affairs at the ASF, stating that the CRA “piles on a whole range of requirements that are either threatening the very fragile ‘win-win’ of open source contributions or our commons, which go against industry good practices or are downright impossible, i.e. it tries to treat the open source commons identical to the commercial sector.”

The Open Source Initiative has compiled responses to the proposed CRA from projects and companies including The Document Foundation (LibreOffice), Python Software Foundation, Electronic Frontier Foundation, RIPE, Linux Foundation, GitHub, Huawei, Microsoft, Sonatype and others expressing concerns. The OpenInfra Foundation remarked that “while the European Commission has tried (through exemptions expressed in recital 10) to protect open source software, it has done so without consulting the

wider open source community during the co-legislative process and therefore has used language that is very likely to have the opposite effect."

Filezilla, providers of a popular file transfer utility, said that "all Open source software operates on a basic principle: producers offer the software freely, but without any liability or warranties for its use. The CRA goes against this principle by imposing unavoidable liability on producers of free software." The project said it would block downloads temporarily in protest.

The legislation has been amended since its first draft, but Mike Milinkovich, Executive Director of the Eclipse Foundation, said in a briefing that while amendments made by the Committee on the Internal Market and Consumer Protection (IMCO) were "positive for open source," those from the ITRE committee which has the lead role are "very worrisome." According to Milinkovich, the ITRE committee has "reached the firm conclusion that most open source projects and all open source foundations should be responsible for CE Mark conformance."

Mozilla has similar concerns, stating that ITRE's amendments mean that "Open source projects with corporate developers as contributors will be subject to the CRA.

Joe Brockmeier, head of community at Percona, told *Dev Class* it was discouraging that the proposed legislation had progressed as far as it has, and voiced concern that in general, despite some voice of opposition from ASF, Eclipse and others, "industry response so far is not robust enough to counter what is likely to be very damaging if it is enacted".

He said the "legislation being considered has been rushed through and has not had sufficient time for affected organizations and individuals to respond. The current draft poses a significant threat to open source software development. Its intended scope and impact is going to threaten open source development, disadvantage smaller players in the market (like Percona), and will likely do more harm than good."

"Open source software development works best when developers are able to collaborate without taking into account employer or nationality. We've seen problems before around encryption and U.S. regulations, as well as restrictions on collaboration with people in sanctioned countries. The EU requiring reporting of vulnerabilities to an EU institution is likely to lead to distorted reporting of security vulnerabilities. Projects that are subject to these restrictions, e.g. those that have European developers, will likely be routed around."

He said it is a "strong possibility" that CRA will "drive some development and participation in open source out of Europe". Brockmeier added: "In the rush to do "something" about security, it's important that we don't destroy or damage a vital commons that serves everyone, equally. If the CRA can't be stopped at this juncture, we must at least seek to ensure it is improved before it's too late."

OpenUK has also heard talk that providers will now simply block their code going into Europe in a similar approach to the way export control is managed," CEO Amanda Brock told us. "This could be deeply damaging to Europe's tech sector. "

She added the EU's continued focus on only giving "carve outs to SME and and failing to do the same for Foundations shows a complete lack of understanding of how open source software works, despite having had an Open Source Program Office for 5 years. The focus on SMEs rather than the nature of open source is extremely short-sighted and feeds into a cycle of perpetuating the lack of growth of European tech companies."

"Setting this super prescriptive framework up won't happen fast and going beyond the appropriateness of what it says, how are these actually going to be implemented? I suspect with great difficulty and very slowly."

The amendments include a provision that "where the main contributors to free and open-source projects are developers employed by commercial entities and when such developers or the employer can exercise control as to which modifications are accepted in the code base, the project should generally be considered to be of a commercial nature." This could apply to many open source projects where employees are given time to contribute. Another concern is that projects which accept "donations… made by commercial entities and… recurring in nature" can be considered commercial. Designation as a commercial activity is critical since the legislation specifies that "only free and open-source software developed or supplied outside made available on the market in the course of a commercial activity should not be covered by this Regulation."

Curbing the cost of cloud analytics and data warehousing

A data language for a full-stack world

Cython 3.0 released after nearly 5 years, but beware breaking changes

Visual Studio preview updates Extension Manager and HTTP Editor, both lag VS Code

Benefits that drive enterprise adoption of graph databases

WordPress Playground: a real-world use for PHP in WebAssembly

New book provides practical help on knowledge graphs for technology professionals

GitHub previews passkeys for no-password authentication, but some would-be adopters struggle

Microsoft hits GA with Dev Box, already in use internally but pricey for the rest of us

Avalonia 11 released: cross-platform framework gets new renderer plus iOS and Android support

AdDuplex shuts down with short notice: Late casualty of Microsoft's Windows Phone and Windows 8 issu...

CommonJS: Here to stay or gone tomorrow?