CYBER SECURITY NEWS · 4 MIN READ

EU Cyber Resilience Act Proposal Requires Controversial 24-Hour Vulnerabi Disclosure

SCOTT IKEDA · OCTOBER 9, 2023

A collection of about a dozen digital rights organizations, including the EFF and Ope Source Initiative, have penned an open letter in opposition to the vulnerability discl terms put forward in the EU's Cyber Resilience Act proposal. Meant to establish strc baseline security standards for "smart" and connected devices, the rights groups fee open source software should be granted certain exemptions to avoid what they see inevitable chilling effect on development due to fears of legal reprisal.

Introduced just over a year ago, the Cyber Resilience Act is still in the process of ping-pong between the two major EU legislative bodies. Parliament Members from the Committee on Industry, Research and Energy backed the draft Cyber Resilience Act in a July vote, but it is unlikely

that any organization will feel its impact for years. If it is eventually codified into law, manufacturers would be given a grace period of two years after adoption to come into compliance under the current terms.

Cyber Resilience Act criticized over requirements for disclosure of unmitigate vulnerabilities

The Cyber Resilience Act attempts to address the persistent problem of smart devic security by adding assorted design and disclosure requirements. The key term that source groups object to is a vulnerability disclosure requirement that would have all manufacturers report to the government within 24 hours of first discovered exploit In most cases, this would mean disclosing before the vulnerability has been mitigate

The digital rights organizations see this as a negative development for device securi Government agencies would end up with large databases full of unmitigated vulnerabilities, something that could either be abused by state intelligence or siphor off by hackers that might be "living off the land" in an agency network. The develop would certainly provide an impetus for hackers to step up their attempts on these agencies, particularly the most state-backed threat groups.

The coalition of rights groups offers several suggestions for modifying the Cyber Resilience Act to address these issues, the first of which is a stipulation that limits tl details that organizations have to provide in vulnerability disclosures to those that c be used to reconstruct it. The groups are also asking for expanded time in which to mitigate if there has not yet been known user harm or a "substantial incident"; it cit reasonable standard period of 90 days. They also call for requirements to formally prohibit government agencies from using reported vulnerabilities for offensive purp and to have strong safety and sharing requirements put in place.

Privacy

Vulnerability disclosure policy likely well-intended, but not properly informed

Some activists and security researchers point out that EU politicians, who very often do not have any kind of IT background, may simply be misunderstanding how the process of

vulnerability disclosure works and what generally accepted best practices are. The government being in possession of the vulnerability information immediately would little to nothing to promote patching, but would increase the amount of vectors by the information might escape or be abused prior to manufacturers being able to complete a good faith effort to issue a patch. The worst case scenario would be a cl public notice from the government well ahead of any mitigation measures being developed, which would be a beacon for the world's malicious hackers to come and advantage of the flaw.

Privacy and open source software advocates also worry that the Cyber Resilience A terms could cripple software development, particularly "white hat" security researc to spotting flaws before they can be exploited by "black hat" actors. Bug bounty pro would be de-incentivized, and even researchers that do work without expectation c compensation would be hampered by more complex reporting processes and greate resistance from organizations.

There is some confusion about the extent to which open source software would be covered by the current Cyber Resilience Act terms. One provision in the bill seems t indicate that not-for-profit open source software would not be subject to the vulnerability disclosure terms, but the definition of "commercial activity" it cites is entirely clear, leaving room for employees or open source foundations that earn mo while contributing to a free project to potentially be subject to the regulation.

Amanda Brock, CEO of OpenUK, expands on this particular concern: "For many yea

Privacy

rce companies and projects have managed legal requirements on expert cc by blocking access to their code for download in those countries. Liability will be created for the entity responsible for 'placing on the market' as the first provider making a digital product available for distribution or use in the EU market in the course of a commercial

activity, whether in return for payment or free of charge. Of course, all open source licences allow for this, so this could easily capture individual developers and not for profits. If the CRA enters into force in its current form, I believe that we can expect projects avoiding the liability which sits with this by blocking access to their produc from their repos and leaving the bigger commercial entities to be the first to distrib the EU. This just cannot be a good position for any country that wants to be recogni as a digital hub or force on the world stage."

George McGregor, VP of Approov, adds that United States developers will also need wary should the Cyber Resilience Act proceed in its current form: "These vulnerabil requirements, if enforced, will be of critical importance to US companies which ope in the EU. The EU Cyber Resilience Act makes no distinction about where vulnerabi are discovered so the obligation will be worldwide in scope. This is clearly understo the number of US based individuals who have signed the request to modify the CRA order to remove the requirement to report unpatched vulnerabilities within 24 hou The letter also requests that vulnerabilities uncovered during testing should not be included in the reporting requirement. With this level of industry reaction, the CRA requirements should certainly be relaxed."

> Proposed EU #CyberResilience Act requires vulnerability disclosure by manufacturers to the government within 24H of first discovered exploitation. In most cases, this would be before the vulnerability has been mitigated. #cybersecurity #respectdata
>
> Click to Pos

Some security researchers have taken the opposite position, however, arguing that criminals are already discovering flaws long before vulnerability disclosures can be and that organizations would likely prefer to be notified as soon as possible so as to the option of taking impacted systems offline before the attack can spread.

TAGS #CYBER RESILIENCE ACT #EU #VULNERABILITY DISCLOSURE

Privacy

Scott Ikeda

Senior Correspondent at CPO Magazine

Scott Ikeda is a technology futurist and writer for more than 15 years. He travels extensively throughout Asia and writes about the impact of technology on the communities he visits. Over the last 5 years, Scott has grown increasingly focused the future landscape of big data, surveillance, cybersecurity and the right to priva

RELATED

Privacy

Privacy

LATEST

Cloudflare: Zero-Day Vulnerability at the Root of Record-Setting DDoS Attack

New California Personal Data Bill Grants State Citizens the Right to Have PII Deleted by Data Brokers

Open Source Software Supply Chain Attacks Have Tripled, But Nearly All Vulnerabilities Are Avoidable by Updating

Hacker Groups Contributing Cyber Attacks to Israel-Hamas Conflict

Privacy

LEARN MORE

About
Contact
Our Advertising
Privacy Policy
Cookie Policy
Terms of Use

STAY UPDATED

Get notified of new articles and relevant events.

Type your email

I agree to the privacy policy

Please verify your request*

I'm not a robot
reCAPTCHA
Privacy - Terms

SUBMIT

LEARN MORE

About
Contact
Our Advertising
Privacy Policy
Cookie Policy
Terms of Use
Do Not Sell My Data

CATEGORIES

Data Privacy
Data Protection
Cyber Security
Tech
Insights
News
Resources
Press Releases

STAY UPDATED

Get notified of new articles and relevant

Type your email

I agree to the privacy policy

Please verify your request*

I'm not a robot

SUBMIT

News, insights and resources for data protection, privacy and cyber security professionals.

Privacy