We, the undersigned organisations, write to express our concern with vulnerability disclosure requirements under the proposed Cyber Resilience Act (CRA). The CRA's objective to encourage software publishers to patch vulnerabilities and report cyber incidents is salutary. However, the CRA's mandatory disclosure of unmitigated vulnerabilities will undermine the security of digital products and the individuals who use them.

The CRA would require organisations to disclose software vulnerabilities to government agencies within 24 hours of exploitation.[1] However, such recently exploited vulnerabilities are unlikely to be mitigated within such a short time, leading to real-time databases of software with unmitigated vulnerabilities in the possession of potentially dozens of government agencies. The more this kind of information is spread, the more likely it is to be misused for state intelligence or offensive purposes, or to be inadvertently exposed to adversaries before a mitigation is in place. In addition, laws that require disclosure of unmitigated vulnerabilities to government agencies create an international precedent that may be reflected by other countries.

We call on you to help improve the CRA by including safeguards that help prevent misuse of vulnerability information:

1. **Limit details.** The regulation should not require disclosure of technical details of unmitigated vulnerabilities to government bodies that would enable another party to reconstruct the vulnerability or develop code to exploit it.
2. **Prohibit offensive uses**. The regulation should include a clear restriction on the use of software vulnerabilities by public bodies, i.e. for intelligence, surveillance, or offensive purposes.
3. **Provide time to mitigate.** In the absence of user harm or a substantial incident, organisations should have a reasonable time to remediate or address the vulnerability before requiring disclosure of its details to governments. A typical standard period for the mitigation of known vulnerabilities is 90 days.
4. **Secure vulnerability information.** Agencies should be obligated to protect vulnerability information with robust security safeguards and shared only on a very strict need-to-know basis.
5. **Protect good faith security researchers.** The regulation should distinguish between vulnerabilities discovered in good faith for defensive purposes and those that are exploited by malicious actors. Good faith security researchers who follow coordinated vulnerability disclosure standards should be protected from retaliation.

We share the goal of strengthening the security of digital products and protecting individuals. The above safeguards will help the CRA achieve its goals of a more resilient and protective technology ecosystem. We appreciate your consideration of our recommendations.

1 Cyber Resilience Act, Articles 11.1, 13.6, 14.4.

Yours sincerely,

Asociatia pentru Tehnologie si Internet – ApTI, Romania
Centre for Democracy & Technology Europe, EU
Eclipse Foundation, EU
Electronic Frontier Foundation (EFF), U.S.
epicenter.works, Austria
European Digital Rights (EDRi), EU
F-Droid, Int'l
Free Software Foundation Europe, EU
Guardian Project, Int'l
Homo Digitalis, Greece
Open Source Initiative, U.S.