21 June 2023

Oversharing is not caring, it is a cyber risk

Joint statement raising concerns on unpatched vulnerability reporting in the Cyber Resilience Act

Vulnerability handling plays a crucial role in maintaining the security and integrity of digital products. By identifying security weaknesses, it allows manufacturers to fix them quickly and effectively.

However, the proposed extension of vulnerability reporting to 'unpatched' vulnerabilities in the Cyber Resilience Act – meaning those to which there is no known fix – will severely harm our collective cybersecurity, rather than enhance it.

We – a diverse coalition of national, European and international associations active across different sectors - ask the European Parliament and Council to remove these obligations, and to instead focus on the reporting of patched vulnerabilities that have been actively exploited and pose a significant cybersecurity risk. As with 'cyber threats' under the NIS2 Directive, manufacturers should, where appropriate, communicate to potentially affected users, especially in a business-to-business context, any measures or remedies they can take in response to a significant vulnerability.

In contrast, reporting unpatched vulnerabilities exposes products to further cyberattacks. In addition, accumulating such sensitive data, be it with ENISA or national authorities, is a cybersecurity risk in itself and will only attract more malicious actors from around the world. For this reason, no other likeminded country has adopted such measures. Established coordinated vulnerability disclosure standards stipulate that vulnerabilities should only be disclosed where mitigation is available.

All signatories are ready to cooperate with the European Parliament and the Council to offer insights and perspectives on the matter, as well as on other ongoing discussions on other articles, to ensure vulnerabilities continue to be handled responsibly to further Europe's cyber protection.

List of signatories

AAVIT, Association for Applied Research in IT, aavit.cz

ACT | The App Association, actonline.org

Adigital, Spanish Association for the Digital Economy, adigital.org

Afnum, French Digital Industry Alliance, afnum.fr

Agoria, agoria.be

AIOTI, Alliance for IoT and Edge Computing Innovation, aioti.eu

ANIS, Romanian Employers' Association of the Software and Services Industry, anis.ro

Anitec-Assinform, anitec-assinform.it

ASD, AeroSpace, Security and Defence Industries Europe, asd-europe.org

BSA – The Software Alliance, bsa.org

CECE, Committee for European Construction Equipment, cece.eu

COCIR, European Coordination Committee of the Radiological Electromedical and Healthcare Information Technology Industry, cocir.org

Cyber Security Coalition, cybersecuritycoalition.org

Danish Chamber of Commerce, danskerhverv.dk

Developers Alliance, developersalliance.org

DI Digital, Danish ICT and Electronics Federation, danskindustri.dk/brancher/di-digital/

DIGITALEUROPE, digitaleurope.org

EGMF, European Garden Machinery Federation, egmf.org

EOS, European Organisation for Security, eos-eu.com

Euralarm, euralarm.org

ESMIG, European Smart Energy Solution Providers, esmig.eu

GZS, Chamber of Commerce and Industry of Slovenia, gzs.si

Hacking Policy Council, centerforcybersecuritypolicy.org/hacking-policy-council

ITI, Information Technology Industry Council, itic.org

ITL, Estonian Association of Information Technology and Telecommunications, itl.ee

JBCE, Japanese Business Council in Europe, jbce.org

Lighting Europe, lightingeurope.org

MedTech Europe, medtecheurope.org

SEMI, semi.org

SEPE, Federation of Hellenic Information Technology & Communications Enterprises, sepe.gr

TechSverige, Swedish IT and Telecom Industries, techsverige.se

Teknikföretagen, Association of Swedish Engineering Industries, teknikforetagen.se

UNIFE, European Rail Supply Industry Association, unife.org

ZIPSEE, Digital Poland Association, cyfrowapolska.org