3rd October 2023

Mr Thierry Breton, Commissioner for Internal Market, European Commission

Ms Carme Artigas Burga, State Secretary for Digitalization and Artificial Intelligence, Ministry of Economic Affairs and Digital Transformation, Spain

Mr. Nicola Danti, Rapporteur for Cybersecurity Resilience Act, European Parliament

As concerned cybersecurity experts who have dedicated our lives to improving the security of the online environment, we urge you to reconsider the vulnerability disclosure requirements under the proposed EU Cyber Resilience Act (CRA). While we appreciate the CRA's aim to enhance cybersecurity in Europe and believe it does indeed do that, we believe that the current provisions on vulnerability disclosure are counterproductive and will create new threats that undermine the security of digital products and the individuals who use them.

Article 11 of the CRA requires software publishers to disclose unpatched vulnerabilities to government agencies within 24 hours of exploitation. This means that dozens of government agencies would have access to a real-time database of software with unmitigated vulnerabilities, without the ability to leverage them to protect the online environment and simultaneously creating a tempting target for malicious actors. There are several risks associated with rushing the disclosure process and having a widespread knowledge of unmitigated vulnerabilities.

Misuse for intelligence and surveillance

Government access to a wide range of unmitigated software vulnerabilities could be misused for intelligence or surveillance purposes. The absence of restrictions on offensive uses of vulnerabilities disclosed through the CRA and the absence of transparent oversight mechanism in almost all EU Member States open the doors to potential misuse.

Risk of exposure to malicious actors

Breaches and the subsequent misuse of government held vulnerabilities are not a theoretical threat but have happened at some of the best protected entities in the world. While the CRA does not require a full technical assessment to be disclosed, even the knowledge of a vulnerability's existence is sufficient for a skilful person to reconstruct it.

Chilling effect on good faith researchers

Disclosing vulnerabilities prematurely may interfere with the coordination and collaboration between software publishers and security researchers, who often need more time to verify, test, and patch vulnerabilities before making them public. As a result, the CRA may reduce the receptivity of manufacturers to vulnerability disclosures from security researchers, and may discourage researchers from reporting vulnerabilities, if each disclosure triggers a wave of government notifications.

While the intention behind disclosing vulnerabilities promptly may be to facilitate mitigation, CRA already requires software publishers to mitigate vulnerabilities without delay in a separate provision. We support this obligation, but also advocate for coordinated disclosure process that balances the need for transparency with the need for security. We recommend that the CRA adopt a risk-based approach to vulnerability disclosure, taking into account factors such as the severity of the vulnerability, the availability of mitigations, the potential impact on users, and the likelihood of broader exploitation. With that in mind and to avoid unintentionally exposing consumers and organisations in Europe and beyond to new cybersecurity risks, we recommend that Article 11, paragraph 1, is either removed in its entirety, or revised as follows:

- Agencies should explicitly be prohibited from using or sharing vulnerabilities disclosed through the CRA for intelligence, surveillance, or offensive purposes.

- Require reporting to agencies of mitigatable vulnerabilities only, within 72 hours of effective mitigations (e.g., a patch) becoming publicly available. Details could include the initial discovery date by the manufacturer.

- The CRA should not require reporting of vulnerabilities that are exploited through good faith security research. In contrast to malicious exploitation of a vulnerability, good faith security research does not pose a security threat.

- Reference ISO/IEC 29147 in Article 11-1 and use it as the baseline for all EU vulnerability reporting.

Signed,

Tony Anscombe, Chief Security Evangelist, ESET

Jaya Baloo, Chief Cybersecurity Officer, Rapid7

Christine Bejerasco, Chief Cybersecurity Officer, WithSecure

Dan Berte, Director of IoT Security, Bitdefender

Anne-Marie Buzatu, Executive Director, ICT4Peace Foundation

Ed Cabrera, Chief Cybersecurity Officer, Trend Micro

Sergio Caltagirone, President, Threat Intelligence Academy

Vint Cerf, VP and Chief Internet Evangelist, Google

Amy Chang, Senior Fellow, Cybersecurity and Emerging Threats, R Street Institute

Jon Clay, Vice President of Threat Intelligence, Trend Micro

John Costello, Deputy Director and Senior Fellow, Wadhwani Center for AI and Advanced Technologies

Peter Dahlen, Managing Director, AmCham Sweden

Christian Dawson, Executive Director, i2Coalition

Ron Deibert, Professor of Political Science and Director, the Citizen Lab at the University of Toronto's Munk School of Global Affairs & Public Policy

Stephane Duguin, Chief Executive Officer, CyberPeace Institute

Casey Ellis, Co-Founder and Chief Technology Officer, Bugcrowd and Co-Founder, Disclose.io Project

Anriette Esterhuysen, Senior Advisor for Internet Governance, Association for Progressive Communications

Ram Ganeshanathan, Vice President of Enterprise Security, Arm

Eva Galperin, Director of Cybersecurity, Electronic Frontier Foundation

Kenneth Geers, Senior Fellow, Atlantic Council and Ambassador for NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Brian Gorenc, Vice President of Threat Research, Trend Micro

Bruce Gustafson, President and Chief Executive Officer, Developers Alliance

Toomas Hendrik Ilves, Former President of Republic of Estonia

Tom Kellermann, Senior Vice President of Cyber Strategy, Contrast Security

Wolfgang Kleinwächter, Professor Emeritus for Internet Policy and Regulation, University of Aarhus

Mallory Knodel, Chief Technology Officer, Center for Democracy and Technology, member of Internet Architecture Board

Olaf Kolkman, Principal Internet Society and former commissioner of the Global Commission on the Stability of Cyberspace

Dr. Ilia Kolochenko, Chief Architect & Chief Executive Officer, ImmuniWeb

Bostjan Koritnik, Deputy Major of the Municipality of Ljubljana, Secretary General of the Association of the Slovenian Lawyers Societies, and former Slovenian Minister for Public Administration

Stephanie Leonard, Head of Government and Regulatory Affairs, TomTom

Ciaran Liam Martin, Professor of Practice in the Management of Public Organisations at the Blavatnik School of Government, University of Oxford

Paul Meyer, Senior Advisor, ICT4Peace

Jeff Moss, Founder of Black Hat and DEF CON Conferences

Katie Moussouris, Founder, Luta Security and Co-author/Co-editor of ISO 29147 and ISO 30111

Chris Painter, President of the GFCE Foundation Board and Former State Department Cyber Coordinator

Bart Preneel, Professor, KU Leuven

Brandon J. Pugh, Director and Senior Fellow for Cybersecurity and Emerging Threats, R Street Institute

Allison Pytlak, Program Lead of the Cyber Program, The Stimson Center

Damir Rajnovic, Cyber Security Manager, Panasonic and former FIRST Board member

Costin Raiu, Independent Researcher; MUTE Group Founding Member and Virus Bulletin Advisory Board Member

Alex Rice, Co-Founder and Chief Technology Officer, HackerOne

Marietje Schaake, Stanford University Cyber Policy Center, Former Member of the European Parliament

Max Smeets, Director of the European Cyber Conflict Research Initiative and a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich

Rayna Stamboliyska, Chief Executive Officer and Founder, RS Strategy - Mastering Uncertainty

Fook Hwa Tan, Chief Quality Officer, Northwave

Jason Turflinger, Managing Director, AmCham Norway

Kayla Underkoffler, Lead Security Technologist, HackerOne

Kristen Verderame, Vice President of Global Government Relations, NetApp

Professor Johanna Weaver, Director of Tech Policy Design Centre, Australian National University

Bill Woodcock, Executive Director, Packet Clearing House

The letter represents the views of the individuals with the names of organizations are included for identification purposes only.