Opinion of the European Cybersecurity Certification Group (ECCG)

on the EUCC Scheme guidance document

"Vulnerability management and disclosure", version 1.0.11, December 2024
Adopted via written procedure on 10 January 2025

The Cybersecurity Act[1] in its Article 62(4), point (e), sets the task for the European Cybersecurity Certification Group (ECCG) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes. Moreover, the European Common Criteria-based cybersecurity certification scheme (EUCC Scheme)[2] in its Articles 48(1) and (2) tasks the ECCG with adopting opinions in view of maintaining the EUCC and to undertake the necessary preparatory works, as well as with adopting opinions endorsing state-of-the-art documents.

ENISA has drafted the EUCC Scheme guidance document "Vulnerability management and disclosure", version 1.0.11 December 2024. This draft guidance document provides requirements for the holder of the EUCC certificate and the IT Security Evaluation Facilities (ITSEF) on how to apply the EUCC. It also includes recommendations for the certification body, for the national cybersecurity certification authorities and recommendations for the Computer Security Incident Response Team designated in the Member State as coordinator for the purposes of coordinated vulnerability disclosure process.

The document has been elaborated with the ENISA Thematic Group on Vulnerability Handling in Certified Solutions (TG VHCS). The ECCG, composed of representatives of Member States, has been consulted and closely involved in developing this draft guidance document, therefore reflecting the opinion of the group. At its meeting on 15 April, the ECCG members agreed to endorse the future final document in the form of a guidance document in view of a possible future state-of-the-art document. The sub-group on EUCC maintenance and review on its meeting on 17 June 2024 discussed the document elaborated by the ENISA TG VHCS.

The ECCG herewith endorses the EUCC Scheme draft guidance document "Vulnerability management and disclosure" version 1.0.11 December 2024 to promote a consistent implementation and enforcement of the provisions of the EUCC in this area, and in view of working further on a possible state-of-the-art document on vulnerability management and disclosure. The ECCG invites the sub-group on EUCC review and maintenance to review the

---

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69.
[2] Commission Implementing Regulation (EU) 2024/482 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC), OJ L, 2024/482, 7.2.2024.

application of the guidance and based on this review, work on a recommendation for a state-of-the art document at the latest on 27th February 2026.

The ECCG invites the sub-group on EUCC review and maintenance to review the application of the guidance at the latest on 27th February 2026 and based on this review, work on a recommendation for a state-of-the art document, at latest by 27th of April 2026.