ENISA Advisory Group

On Common Vulnerabilities and Exposures (CVE)

June 2025

AUTHORS

Sebastiaan van't Erve, Ilias Chantzos, Jos Helmich, Stephane Lenco, Bart Preneel, Annita Sciacovelli, Thomas Tschersich, Csaba Virag, Zeina Zakhour

ACKNOWLEDGEMENTS

Main drafting lead by Sebastiaan van 't Erve

DISCLAIMER

The opinions expressed by the Advisory Group (AG) are not binding on the European Union Agency for Cybersecurity (ENISA) and do not represent the official position of the Agency. ENISA accepts no responsibility for any opinions or statements made by the AG.

1. INTRODUCTION

The Advisory Group of the European Network and Information Security Agency (ENISA), comprising of cybersecurity experts from institutions, academia, civil society and industry, has observed the recent developments regarding the Common Vulnerabilities and Exposures (CVE) framework. The Advisory Group deems it important and urgent to express its opinion to support the Executive Director as to how ENISA can contribute to the strengthening of the global vulnerability ecosystem.

The availability, stability and continuity of the CVE framework is a matter of global importance. The functioning of the global vulnerability ecosystem is conditional for the ambitions of Europe's Digital Decade. Transparency about existing vulnerabilities is key for granting security of our digital markets and European sovereignty.

The Advisory Group is of the opinion that based on the Network and Information Security Directive 2 (NIS2) it is justified to conclude that the current CVE framework is the de facto international standard that represents the best practice for the referencing of vulnerabilities and that cooperation between the CVE framework and the recently created European Vulnerabilities Database (EUVD) should be maximised as the NIS2 directive clearly states:

> *"Whereas,*
>
> *(59)*
>
> *The Commission, ENISA and the Member States should continue to foster alignments with international standards and existing industry best practices in the area of cybersecurity risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.*
>
> *(63)*
>
> *(…) In order, to the extent possible, to avoid a duplication of efforts and to seek complementarity, ENISA should explore the possibility of entering into structured cooperation agreements with similar registries or databases that fall under third-country jurisdiction. In particular, ENISA should explore the possibility of close cooperation with the operators of the Common Vulnerabilities and Exposures (CVE) system."*

2. RECOMMENDATIONS

Based on the enduring uncertainties concerning the CVE framework and the specific wording of the NIS2 Directive we formulate the following four recommendations[1]:

Recommendation 1: Actively explore whether ENISA can become a 'Top-Level Root' in the CVE framework for the territory of the European Union.

Becoming a Top-Level Root will give ENISA a bi-directional flow between the EUVD and CVE databases, thus ensuring better synchronicity in the global vulnerability ecosystem.

Recommendation 2: Actively strive for a seat in the governing body of the CVE-framework

As the governance of the CVE framework evolves, the EU through ENISA should apply for a chair in the likely body overseeing the CVE framework to propose the changes that will ensure EUVD/CVD coordination, such as the inclusion of default vulnerable configurations as a vulnerability of its own, or the operationalization of the Root-CNA programme still largely in its infancy.

Recommendation 3: Urgently organise the necessary resources

It is a matter of digital sovereignty for the European Union to be able to handle vulnerabilities on its own. The Advisory Group encourages The Commission, ENISA and the Member States to take bold action to organise the necessary resources in the shortest time possible.

Recommendation 4: Engage all European stakeholders

The Advisory Group strongly encourages ENISA to actively engage all European stakeholders, ranging from civil society, academia to industry and from national to European institutions, in this fundamental evolution of vulnerability handling globally and its incarnation in the European Union as a role model.

[1] As decided during the meeting of the Advisory Group in Athens, Greece on the 27th of June 2025.